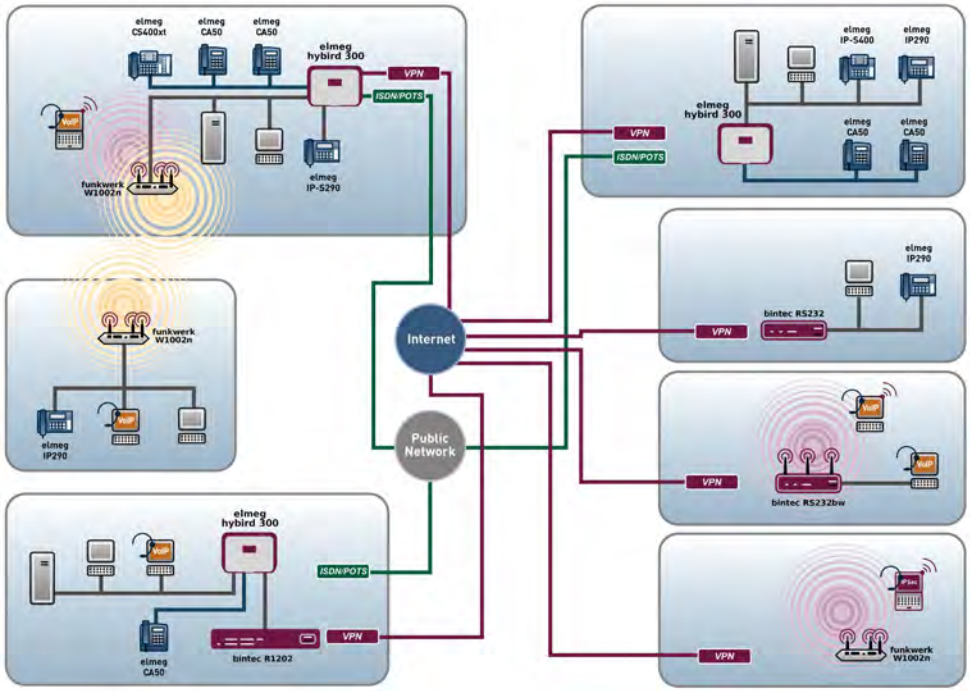


Manual
bintec WLAN and Industrial WLAN

Reference

Copyright© Version 9.0, 2010 Funkwerk Enterprise Communications GmbH

Legal Notice

Aim and purpose
This document is part of the user manual for the installation and configuration of funkwerk devices. For the latest information and notes on the current software release, please also read our release notes, particularly if you are updating your software to a higher release version. You will find the latest release notes under *www.funkwerk-ec.com* .

Liability
This manual has been put together with the greatest possible care. However, the information contained in this manual is not a guarantee of the properties of your product. Funkwerk Enterprise Communications GmbH is only liable within the terms of its conditions of sale and supply and accepts no liability for technical inaccuracies and/or omissions.

The information in this manual can be changed without notice. You will find additional information and also release notes for funkwerk devices under *www.funkwerk-ec.com* .

Funkwerk devices make WAN connections as a possible function of the system configuration. You must monitor the product in order to avoid unwanted charges. Funkwerk Enterprise Communications GmbH accepts no responsibility for data loss, unwanted connection costs and damage caused by unintended operation of the product.

Trademarks
funkwerk trademarks and the funkwerk logo, bintec trademarks and the bintec logo, artem trademarks and the artem logo, elmeg trademarks and the elmeg logo are registered trademarks of Funkwerk Enterprise Communications GmbH.

Company and product names mentioned are usually trademarks of the companies or manufacturers concerned.

Copyright
All rights reserved. No part of this manual may be reproduced or further processed in any way without the written consent of Funkwerk Enterprise Communications GmbH. The documentation may not be processed and, in particular, translated without the consent of Funkwerk Enterprise Communications GmbH.

You will find information on guidelines and standards in the declarations of conformity under *www.funkwerk-ec.com* .

How to reach Funkwerk Enterprise Communications GmbH
Funkwerk Enterprise Communications GmbH, Südwestpark 94, D-90449 Nuremberg, Germany, Phone: +49 911 9673 0, Fax: +49 911 688 07 25
Funkwerk Enterprise Communications France S.A.S., 6/8 Avenue de la Grande Lande, F-33174 Gradignan, France, Phone: +33 5 57 35 63 00, Fax: +33 5 56 89 14 05
Internet: *www.funkwerk-ec.com*

Table of Contents

Chapter 1 Introduction 1

Chapter 2 About this guide. 3

Chapter 3 Installation. 6

3.1 Setting up and connecting 6

3.2 Cleaning. 12

3.3 Support information 13

Chapter 4 Basic configuration 14

4.1 Presettings 14

4.1.1 Preconfigured data 14

4.1.2 Software update 15

4.2 System requirements 16

4.3 Preparations 16

4.3.1 Gathering data 16

4.3.2 Configuring a PC 18

4.4 IP configuration. 19

4.5 Modify system password. 22

4.6 Setting up a wireless network 22

4.7 Setting up a bridge link 23

4.8 Software Update 24

Chapter 5 Reset 26

Chapter 6 Technical data 28

6.1 Scope of supply 28

6.2 General Product Features 30

6.3 LEDs 39

6.4 Connectors 43

6.5 Antenna connectors for industrial WLAN devices with 802.11n support . 45

6.6 Pin Assignments 46

6.6.1 Ethernet interface 46

6.6.2 Serial interface 47

6.6.3 Socket for power supply 47

6.7 Frequencies and channels 48

6.8 WEEE information 49

Chapter 7 Access and configuration 50

7.1 Access Options 50

7.1.1 Access via LAN 50

7.1.2 Access via the Serial Interface 53

7.2 Logging in 55

7.2.1 User names and passwords in ex works state 55

7.2.2 Logging in for Configuration 56

7.3 Configuration options 56

7.3.1 Funkwerk Configuration Interface for advanced users 57

7.3.2 SNMP shell 72

7.4 BOOTmonitor 72

Chapter 8 Assistants 74

Chapter 9 System Management 75

9.1 Status 75

9.2 Global Settings 78
9.2.1 System 78
9.2.2 Passwords 80
9.2.3 Date and Time 82
9.2.4 System Licences 86

9.3 Interface Mode / Bridge Groups 89
9.3.1 Interfaces 91

9.4 Administrative Access 94
9.4.1 Access 95
9.4.2 SSH 96
9.4.3 SNMP 100

9.5 Remote Authentication 101
9.5.1 RADIUS 101
9.5.2 TACACS+ 107
9.5.3 Options 110

9.6 Certificates 112
9.6.1 Certificate List 112
9.6.2 CRLs 121
9.6.3 Certificate Servers 122

Chapter 10 Physical Interfaces 124

10.1 Ethernet Ports 124
10.1.1 Port Configuration 124

10.2 Serial Port 126
10.2.1 Serial Port 126

10.3 Relay 130

10.3.1 Relay Configuration 131

Chapter 11 LAN 132

11.1 IP Configuration 132
11.1.1 Interfaces 132

11.2 VLAN 136
11.2.1 VLANs 138
11.2.2 Port Configuration 139
11.2.3 Administration 140

Chapter 12 Wireless LAN 141

12.1 WLAN 142
12.1.1 Radio Settings 142
12.1.2 Virtual Service Sets 155
12.1.3 WDS Links 162
12.1.4 Client Link 165
12.1.5 Bridge Links 169

12.2 Administration 177
12.2.1 Basic Settings 177

Chapter 13 Wireless LAN Controller 179

13.1 Wizard 179
13.1.1 Basic Setup 179
13.1.2 Wireless Radio Profiles 180
13.1.3 Wireless Networks 180
13.1.4 Start automatic installation 183

13.2 Controller Configuration 184
13.2.1 General 185

13.3 Slave AP Configuration 186

13.3.1 Slave Access Points . . . 187
13.3.2 Radio Modules . . . 189
13.3.3 Radio Profiles . . . 192
13.3.4 Wireless Networks (VSS) . . . 199

13.4 Monitoring . . . 204
13.4.1 Active Clients . . . 205
13.4.2 Neighbor APs . . . 206

13.5 Maintenance . . . 206
13.5.1 Firmware Maintenance . . . 207

Chapter 14 Routing . . . 209

14.1 Routes . . . 209
14.1.1 IP Routes . . . 209
14.1.2 Options . . . 214

14.2 NAT . . . 216
14.2.1 NAT Interfaces . . . 216
14.2.2 NAT Configuration . . . 218

14.3 RIP . . . 223
14.3.1 RIP Interfaces . . . 223
14.3.2 RIP Filter . . . 226
14.3.3 RIP Options . . . 228

14.4 Load Balancing . . . 231
14.4.1 Load Balancing Groups . . . 231

14.5 Multicast . . . 233
14.5.1 Forwarding . . . 235
14.5.2 IGMP . . . 236
14.5.3 Options . . . 239

14.6 QoS . . . 241
14.6.1 QoS Filter . . . 241
14.6.2 QoS Classification . . . 244

14.6.3 QoS Interfaces/Policies 246

Chapter 15 WAN 253

15.1 Internet + Dialup 253
15.1.1 PPPoE 255
15.1.2 PPTP 259
15.1.3 IP Pools 264

15.2 Real Time Jitter Control 265
15.2.1 Controlled Interfaces 265

Chapter 16 VPN 268

16.1 IPSec 268
16.1.1 IPSec Peers 268
16.1.2 Phase-1 Profiles 274
16.1.3 Phase-2 Profiles 281
16.1.4 XAUTH Profiles 285
16.1.5 IP Pools 288
16.1.6 Options 289

16.2 L2TP 292
16.2.1 Tunnel Profiles 292
16.2.2 Users 296
16.2.3 Options 302

16.3 GRE 303
16.3.1 GRE Tunnels 303

Chapter 17 Firewall 306

17.1 Policies 307
17.1.1 Filter Rules 308
17.1.2 QoS 311
17.1.3 Options 313

17.2 Interfaces . . . 315
17.2.1 Groups . . . 315
17.3 Addresses . . . 316
17.3.1 Address List . . . 316
17.3.2 Groups . . . 317
17.4 Services . . . 318
17.4.1 Service List . . . 318
17.4.2 Groups . . . 320

Chapter 18 Local Services . . . 322

18.1 DNS . . . 322
18.1.1 Global Settings . . . 324
18.1.2 Static Hosts . . . 327
18.1.3 Domain Forwarding . . . 328
18.1.4 Cache . . . 330
18.1.5 Statistics . . . 332
18.2 HTTPS . . . 333
18.2.1 HTTPS server . . . 333
18.3 DynDNS Client . . . 334
18.3.1 DynDNS Update . . . 335
18.3.2 DynDNS Provider . . . 336
18.4 DHCP Server . . . 338
18.4.1 DHCP Pool . . . 339
18.4.2 IP/MAC Binding . . . 341
18.4.3 DHCP Relay Settings . . . 342
18.5 Scheduling . . . 343
18.5.1 Schedule . . . 344
18.5.2 Options . . . 347
18.6 Surveillance . . . 348

18.6.1 Hosts . . . 348
18.6.2 Interfaces . . . 350
18.6.3 Temperature . . . 352
18.6.4 Ping Generator . . . 354
18.7 Funkwerk Discovery . . . 355
18.7.1 Device Discovery . . . 355
18.7.2 Options . . . 359
18.8 Hotspot Gateway . . . 359
18.8.1 Hotspot Gateway . . . 361

Chapter 19 Maintenance . . . 367

19.1 Diagnostics . . . 367
19.1.1 Ping Test . . . 367
19.1.2 DNS Test . . . 368
19.1.3 Traceroute Test . . . 368
19.2 Software & Configuration . . . 369
19.2.1 Options . . . 369
19.3 Reboot . . . 374
19.3.1 System Reboot . . . 374

Chapter 20 External Reporting . . . 375

20.1 Syslog . . . 375
20.1.1 Syslog Servers . . . 375
20.2 IP Accounting . . . 378
20.2.1 Interfaces . . . 378
20.2.2 Options . . . 379
20.3 E-mail Alert . . . 380
20.3.1 E-mail Alert Server . . . 380
20.3.2 E-mail Alert Recipient . . . 382

20.4 SNMP . . . 383
20.4.1 SNMP Trap Options . . . 384
20.4.2 SNMP Trap Hosts . . . 385
20.5 Activity Monitor . . . 386
20.5.1 Options . . . 387

Chapter 21 Monitoring . . . 389

21.1 Internal Log . . . 389
21.1.1 System Messages . . . 389
21.2 IPSec . . . 390
21.2.1 IPSec Tunnels . . . 390
21.2.2 IPSec Statistics . . . 392
21.3 Interfaces . . . 394
21.3.1 Statistics . . . 394
21.4 WLAN . . . 396
21.4.1 WLAN1 . . . 396
21.4.2 VSS . . . 398
21.4.3 WDS . . . 401
21.4.4 Bridge Links . . . 404
21.4.5 Client Links . . . 406
21.5 Bridges . . . 408
21.5.1 br<x> . . . 408
21.5.2 sta<x> . . . 409
21.6 Hotspot Gateway . . . 410
21.6.1 Hotspot Gateway . . . 410
21.7 QoS . . . 411
21.7.1 QoS . . . 411

Index . . . 412

Chapter 1 Introduction

The new generation access points are manufactured in an environmentally friendly way and meet the RoHS directive. They support the latest WLAN technology and are designed for use particularly in the professional environment.

Safety notices

The **safety precautions** brochure, which is supplied with your device, tells you what you need to take into consideration when using your access point.

Installation

How to connect your device is shown in chapter *Installation* on page 6.

Configuration

Chapter *Basic configuration* on page 14 also tells you what preliminary tasks are necessary for configuration. You will then be shown how you can access your device from a Windows PC using a current web browser and how to make basic settings.

Password

If you are familiar with the configuration of **bintec** devices and you want to get started right away, all you really need to know is the preset user name and password.

User Name: `admin`

Password: `funkwerk`

Note

Remember to change the password immediately when you log in to the device for the first time. All **bintec** devices are supplied with the same password, which means they are not protected against unauthorised access until you change the password. How to change the passwords is described in chapter *Modify system password* on page 22.

Workshops

Step-by-step instructions for the most important configuration tasks can be found in the separate **FEC Application Workshop** guide for each application, which can be downloaded from the *www.funkwerk-ec.com* website under **Solutions**.

WLAN Management

The devices are designed for use with **WiLMA**. **WiLMA**, the WLAN management solution from Funkwerk, offers a software application in a client/server architecture that allows you to centrally monitor, control and maintain all Funkwerk access points in medium and large wireless LANs.

Dime Manager

The devices are also designed for use with **Dime Manager**. The **Dime Manager** management tool can locate your bintec devices within the network quickly and easily. The .NET-based application, which is designed for up to 50 devices, offers easy to use functions and a comprehensive overview of devices, their parameters and files.

All devices in the local network, including remote devices that can be reached over SNMP, are located using SNMP Multicast irrespective of their current IP address. A new IP address and password and other parameters can also be assigned. A configuration can then be initiated over HTTP or TELNET. If using HTTP, the Dime Manager automatically logs into the devices on your behalf.

System software files and configuration files can be managed individually as required or in logical groups for devices of the same type.

You can find the **Dime Manager** on the enclosed product DVD.

Chapter 2 About this guide

This document is valid for **bintec** devices with system software as of software version 7.9.5.

The guide, which you have in front of you, contains the following chapters:

User's Guide - Reference

Chapter	Description
Introduction	You see an overview of the the device:
About this guide	We explain the various components of this manual and how to use it.
Installation	This contains instructions for how to set up and connect your device.
Basic configuration	This chapter provides a step-by-step guide to the basic functions on your device.
Reset	This chapter explains how to reset your device to the ex works state.
Technical data	This section contains a description of all the device's technical properties.
Access and configuration	This includes explanations about the different access and configuration methods.
Assistants System management Physical Interfaces LAN Wireless LAN Wireless LAN Controller Routing WAN VPN Firewall	These chapters describe all configuration options of the **Funkwerk Configuration Interface**. The individual menus are described in the order of navigation. The individual chapters also contain more detailed explanations on the subsystem in question.

Chapter	Description
Local Services Maintenance External Reporting Monitoring	
Glossary	The glossary contains a reference to the most important technical terms used in network technology.
Index	The index lists all the key terms for operating the device and all the configuration options and gives page numbers so they can be found easily.

To help you locate information easily, this user's guide uses the following visual aids:

List of visual aids

Icon	Use
	Indicates practical information.
	Indicates general and important points.
	Indicates a warning of risk level "Attention" (points out possible dangers that may cause damage to property if not observed).
	Indicates a warning of risk level "Warning" (points out possible dangers that may cause physical injury or even death if not observed).

The following typographical elements are used to help you find and interpret the information in this user's guide:

Typographical elements

Typographical element	Use
•	Indicates lists.
Menu -> **Submenu** **File** -> **Open**	Indicates menus and sub-menus.
non-proportional, e.g.	Indicates commands that you must enter as written.

Typographical element	Use
`ping 192.168.1.254`	
bold, e.g. **Windows Start menu**	Indicates keys, key combinations and Windows terms.
bold, e.g. **Licence Key**	Indicates fields.
italic, e.g. *none*	Indicates values that you enter or that can be configured.
Online: blue and italic, e.g. *www.funkwerk-ec.com*	Indicates hyperlinks.

Chapter 3 Installation

Note

Please read the safety notices carefully before installing and starting up your device. These are supplied with the device.

Refer to chapter *Technical data* on page 28.

3.1 Setting up and connecting

Note

All you need for this are the cables and antennas supplied with the equipment.

The device can be fitted with various antenna systems. External, screw-on standard antennas can be used (optional).

The access points of the outdoor version (**bintec WIx065n**) can be mounted on a mast or DIN rail (indoor version only). Optional theft protection is also available for the indoor and outdoor versions.

For the **bintec WI** series devices, a screw terminal bar is included as standard for power supply.

Devices of the industrial WLAN series with 802.11n support are fitted with a unit that heats the radio module to operating temperature when the temperature falls below 10 degrees Celsius. Once this temperature has been reached, the device continues with the start-up process. During the heating phase the red Failure LED flashes.

Caution

The use of the wrong mains adapter may damage your device. Only use the mains adaptor supplied (only for **bintec W1002n**). If you require foreign adapters/mains units, please contact our funkwerk service.

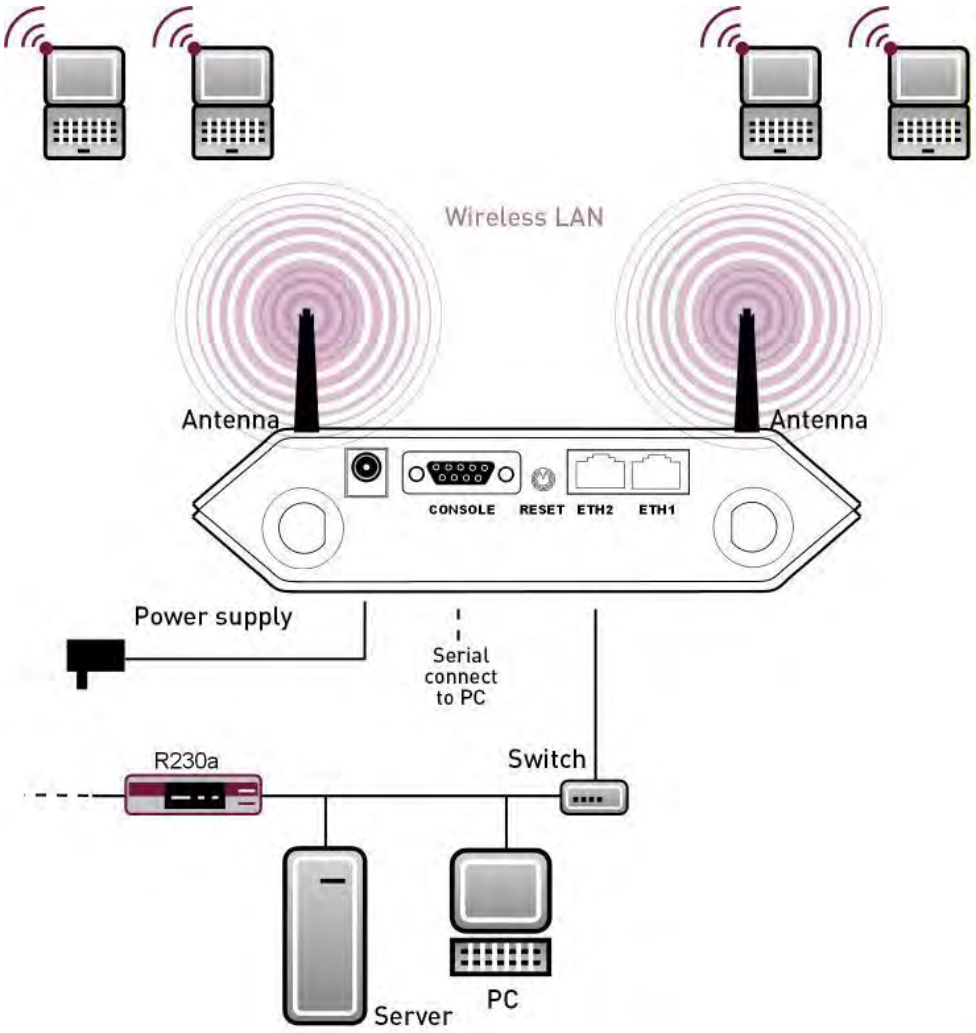


Fig. 2: Connection options **bintec W1002n**

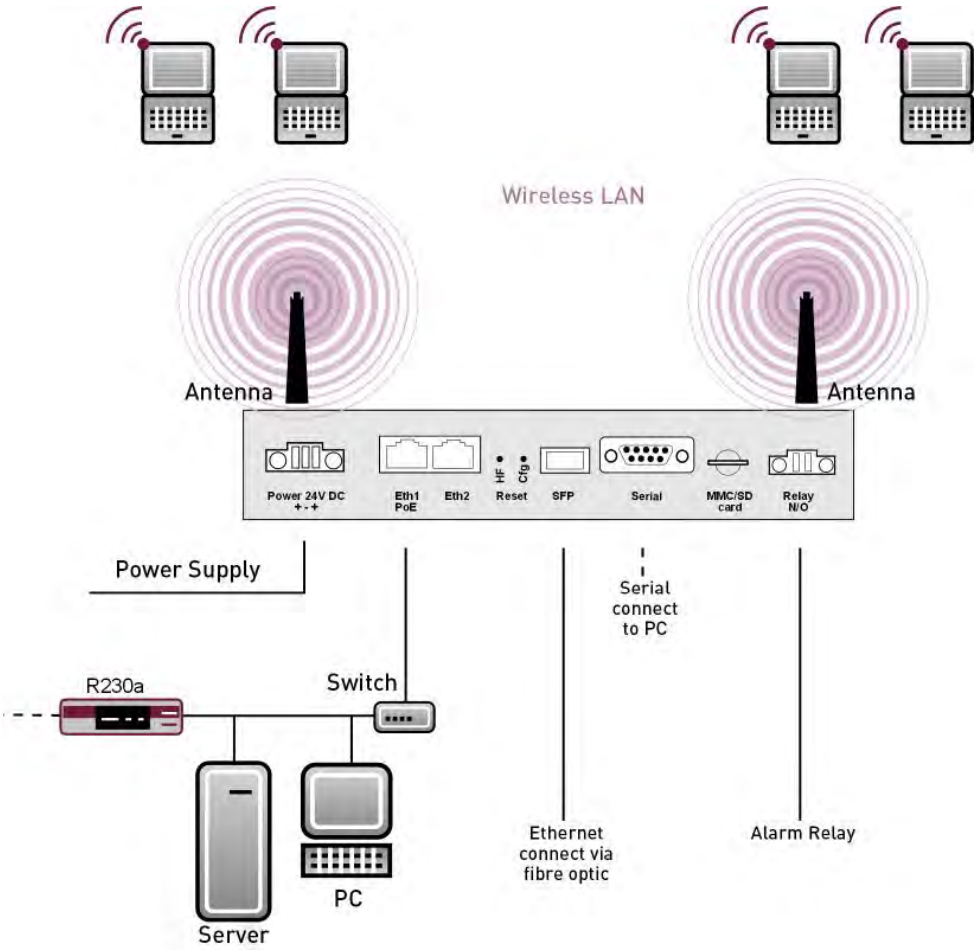


Fig. 3: Connection options **bintec WIx040n** *and* **bintec WIx065n**.

When setting up and connecting, carry out the steps in the following sequence (refer to the connection diagrams for the individual devices in chapter *Technical data* on page 28):

(1) Antennas

Screw the standard antennas supplied on to the connectors provided for this purpose.

Put the antennas in the required position before tightening the screw nut. Once the screw nut has been tightened, it may not be possible to rotate the radiator any more.

If two antennas are connected to the device, these must be installed at least 6 cm and preferably 12 cm apart so that antenna diversity can be used.

In highly reflective environments, it may make sense to maintain an angle of 90° in the direction of the antennas. For this, arrange the antennas in a V shape.

(2) Installation

The access points can be fitted to the wall using brackets on the housing or can

used as a table-top device.

Wall mounting

To attach the device to the wall, use the brackets on the back of the housing. Optional wall mounting with theft protection is available.

Warning

Before drilling, make sure that there are no building installations where you are drilling. If gas, electricity, water or waste water lines are damaged, you may endanger your life or damage property.

- Screw the mount to the wall with the 2 screws.
- Hang the device in the mount with the screw nut but do not tighten it. Make sure the device connections are accessible.
- Protect the device against theft with the lock supplied.

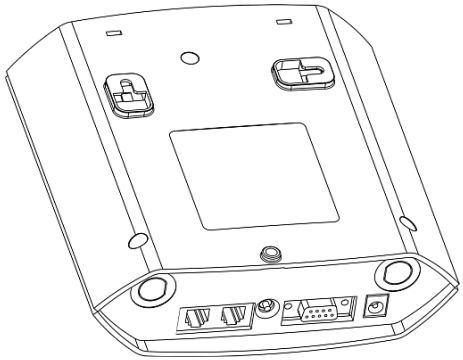


Fig. 4: Wall mounting straps **bintec W1002n**

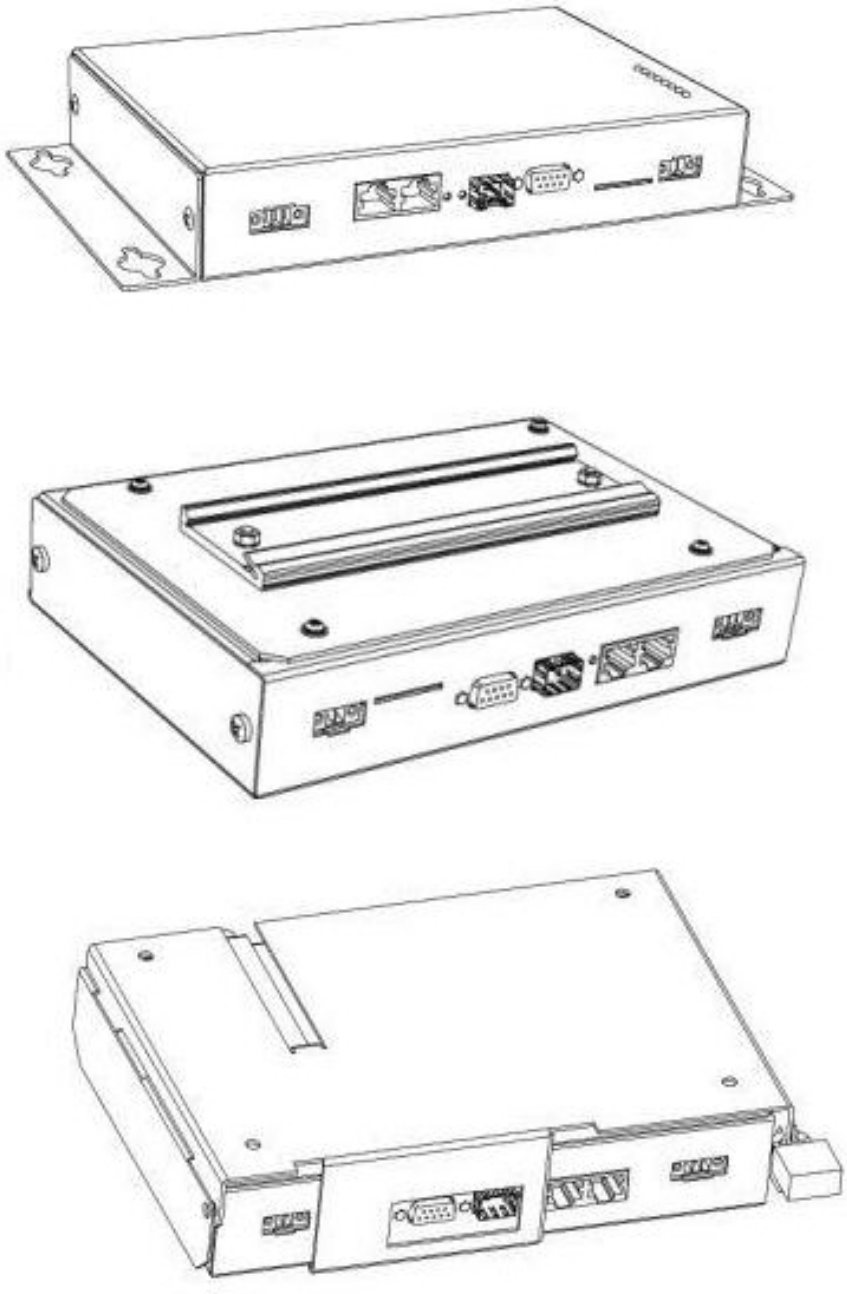


Fig. 5: Wall mounting of the **bintec WIx040n** *(standard design, DIN rail or theft protection optional)*

Fig. 6: Wall mounting of the **bintec WIx065n** *(standard design and with theft protection)*

Use as a table-top device

The access point can also be used as a table-top device. For this option, use the four self-adhesive feet on the bottom of the device. Place your device on a solid, level base.

(3) LAN

For the standard configuration of your device via Ethernet, connect port **ETH1** or **ETH2** of your device to your LAN using the Ethernet cable supplied. The device automatically detects whether it is connected to a switch or directly to a PC.
Use just one of the ports **ETH1** and **ETH2**, the second port is used to cascade a number of devices. If you use both Ethernet connections on the same switch, loops may be formed.
The standard patch cable (RJ45-RJ45) is symmetrical. It is therefore not possible to mix up the cable ends.

(4) Power connection

Connect the device to a mains socket using the mains adaptor supplied.
Use the power cord supplied (or the screw strip terminal in the case of the WI series) and insert it in the appropriate socket on your device. Now plug the power cord into a power socket (100–240 V). The status LEDs signal that your device is correctly connected to the power supply.

Note

WI series products are supplied without a mains unit. All devices must be earthed.

Note

To restrict power in the event of a fault, the 24 V DC electric circuit is to be protected with an external 2 A fuse on the installation side for **bintec WIx040n** and **bintec WIx065n**. The relay contact must also be protected externally with a 1-A fuse (AC) or 2-A fuse (DC).

Note

If the **bintec WIx065n** is installed outdoors, the lines laid outside the building are to be categorized as TNV1 electric circuits in accordance with EN60950, as their SELV level can also be overridden by transient overvoltage (e.g. during storms) during operation in line with the regulations. When wiring the connections, it is therefore necessary to make sure that protective measures against overvoltage are carried out where the cable enters the building, to ensure that the limit values of a SELV electric circuit are maintained in the building.

You can set up further connections as required:

- Serial connection: For alternative configuration possibilities, connect the serial interface of your PC (**COM1** or **COM2**) to the serial interface of the gateway (**console**). However, configuration via the serial interface is not provided by default.

Note

Note that the serial interface of **bintec WIx065n** must only be used by a service technician as a maintenance interface.

The device is now ready for configuration.

3.2 Cleaning

You can clean your device easily. Use a damp cloth or antistatic cloth. Do not use solvents. Never use a dry cloth; the electrostatic charge could cause electronic faults. Make sure that no moisture can enter the device and cause damage.

3.3 Support information

If you have questions about your product or are looking for additional information, the Funkwerk Enterprise Communications GmbH Support Centre can be reached Monday to Friday between the hours of 8.00 am and 5 pm. They can be contacted as follows:

Email	hotline@funkwerk-ec.com
International Support Coordination	Telephone: +49 911 9673 1550 Fax: +49 911 9673 1599
End-customer Hotline	0900 1 38 65 93 (€1.10/min on land-lines in Germany)

For detailed information on our support services, contact *www.funkwerk-ec.com*.

Chapter 4 Basic configuration

You can use the **Dime Manager** (IP address assignment) and the **Funkwerk Configuration Interface** (other configuration steps) for the basic configuration of your device.

The basic configuration is explained below step-by-step. A detailed online help system gives you extra support.

This user's guide assumes you have the following basic knowledge:

- Basic knowledge of network structure
- Knowledge of basic network terminology, such as server, client and IP address
- Basic knowledge of using Microsoft Windows operating systems

The **Companion DVD** also supplied includes all the tools that you need for the configuration and management of your device.

You can find other useful applications on the Internet at *www.funkwerk-ec.com* .

4.1 Presettings

4.1.1 Preconfigured data

You have three ways of accessing your device in your network to perform configuration tasks:

(a) Dynamic IP address

In ex works state, your device is set to DHCP client mode, which means that when it is connected to the network, it is automatically assigned an IP address if a DHCP server is run. You can then access your device for configuration purposes using the IP address assigned by the DHCP server. For information on determining the dynamically assigned IP address, please see your DHCP server documentation.

(b) Fallback IP address

If you do not run a DHCP server, you can connect your device directly to your configuration PC and then reach it using the following, predefined fallback IP configuration:

- **IP Address**: `192.168.0.252`
- **Netmask**: `255.255.255.0`

Make sure that the PC from which the configuration is performed has a suitable IP

configuration (see *Configuring a PC* on page 18).

(c) Assigning a fixed IP address

You can use the **Dime Manager** to assign a new IP address and the required password to your device.

Note

Please note:

If your device has obtained an IP address dynamically from a DHCP server operated in your network for the basic configuration, the fallback IP address 192.168.0.252 is deleted automatically and your device will no longer function over this address.

However, if you have set up a connection to the device over the fallback IP address 192.168.0.252 or have assigned an IP address with the **Dime Manager** in the basic configuration, you will only be able to access your device over this IP address. The device will no longer obtain an IP configuration dynamically over DHCP.

Use the following access data to configure your device in an ex works state:

- **User Name**: `admin`
- **Password**: `funkwerk`

Note

All **bintec** devices are delivered with the same username and password. As long as the password remains unchanged, they are therefore not protected against unauthorised use. Make sure you change the passwords to prevent unauthorised access to your device!

How to change the passwords is described in *Modify system password* on page 22.

4.1.2 Software update

Your device contains the version of the system software available at the time of production. More recent versions may have since been released. You can easily perform an update with the **Funkwerk Configuration Interface** using the **Maintenance** -> **Software & Configuration** menu.

For a description of the update procedure, see *Software Update* on page 24.

4.2 System requirements

For configuration, your PC must meet the following system requirements:

- Microsoft Windows operating system Windows 2000 or higher
- Internet Explorer 6 or 7, Mozilla Firefox Version 1.2 or higher
- Installed network card (Ethernet)
- DVD drive
- TCP/IP protocol installed (see *Configuring a PC* on page 18)
- High colour display (more than 256 colours) for correct representation of the graphics.

4.3 Preparations

To prepare for configuration, you need to...

- Obtain the data required for the basic configuration.
- Check whether the PC from which you want to perform the configuration meets the necessary requirements.
- Install the **Dime Manager** software, which provides more tools for working with your device.

4.3.1 Gathering data

The main data for the basic configuration can be gathered quickly, as no information is required that needs in-depth network knowledge. If applicable, you can use the example values.

Before you start the configuration, you should gather the data for the following purposes:

- IP configuration (obligatory if your device is in the ex works state)
- Optional: Configuration of a wireless network connection in Access Point mode
- Optional: Configuration of client links in Client Links mode
- Optional: Configuration of bridge links in Bridge mode.

The following table shows examples of possible values for the necessary data. You can enter your personal data in the "Your values" column, so that you can refer to these values later when needed.

If you configure a new network, you can use the given example values for IP addresses

and netmasks. In cases of doubt, ask your system administrator.

Basic configuration

For a basic configuration of your gateway, you need information that relates to your network environment:

IP configuration of the access point

Access data	Example value	Your values
IP address of your access point	*192.168.0.252*	
Netmask of your access point	*255.255.255.0*	

Access Point mode

If you run your device in Access Point mode, you can set up the required wireless networks. To do this, you need the following data:

Configuration of a wireless network

Access data	Example value	Your values
Network Name (SSID)	*Funkwerk-ec*	
Security mode	*WPA-PSK*	
Preshared Key	*supersecret*	

Access Client mode

If you run your device in Access Client mode, you can set up the required client links. To do this, you need the following data:

IP configuration of the access client

Access data	Example value	Your values
Network Name (SSID)	*Funkwerk-ec*	
Security mode	*WPA-PSK*	
Preshared Key	*supersecret*	

Bridge mode

If you run your device in Bridge mode, you can either configure connections to other bridges manually or use the bridge link autoconfiguration function. For the manual configuration of a bridge link, you need the following data:

Configuration of a bridge link

Access data	Example value	Your values
Preshared Key	*bridgesecret*	
MAC address of remote bridge	*00:a0:f9:5a:42:53*	

To use the bridge link autoconfiguration function, proceed as described in the **Automatic Configuration of a Bridge Link** workshop and read the **Wireless LAN** chapter of the user's guide under **WLAN** -> **Bridge Links** -> **Add**.

4.3.2 Configuring a PC

In order to reach your device via the network and to be able to carry out configuration, the PC used for the configuration has to satisfy some prerequisites.

- Make sure that the TCP/IP protocol is installed on the PC.
- Select the suitable IP configuration for your configuration PC.

  The PC via which you want to configure the IP address for your device must be in the same network as your device.

Checking the Windows TCP/IP protocol

Proceed as follows to check whether you have installed the protocol:

(1) Click the Windows Start button and then **Settings** -> **Control Panel** -> **Network Connections** (Windows XP) or **Control Panel** -> **Network and Sharing Center**-> **Change Adapter Settings** (Windows 7).

(2) Click on **LAN Connection**.

(3) Click on **Properties** in the status window.

(4) Look for the **Internet Protocol (TCP/IP)** entry in the list of network components.

Installing the Windows TCP/IP protocol

If you cannot find the **Internet Protocol (TCP/IP)** entry, install the TCP/IP protocol as follows:

(1) First click **Properties**, then **Install** in the status window of the **LAN Connection**.

(2) Select the **Protocol** entry.

(3) Click **Add**.

(4) Select **Internet Protocol (TCP/IP)** and click on **OK**.

(5) Follow the on-screen instructions and restart your PC when you have finished.

Allocating PC IP address

Allocate an IP address to your PC as follows:

(1) Select **Internet Protocol (TCP/IP)** and click on **Properties**.

(2) Choose **Use following IP address** and enter a suitable IP address, the matching netmask, your default gateway and your preferred DNS server.

If you run a DHCP server in your network, you can apply the default Windows setting **Obtain IP address automatically** and **Obtain DNS server address automatically**.

Your PC should now meet all the prerequisites for the configuration of your device.

4.4 IP configuration

In the ex works state, your device is configured in DHCP Client mode and therefore dynamically receives an IP address if you run a DHCP server in your network. If this is not the case, connect your device directly to the configuration PC and use the fallback IP address *192.168.0.252*.

Alternatively, you can assign your device the required fixed IP address by using the **Dime Manager**.

To do this, install the program from the DVD provided on your configuration PC.

Proceed as follows:

(a) Place the DVD provided in the DVD drive of your configuration PC. The installation wizard should start automatically. If it does not, open the following file on the DVD using your file browser: `starter.exe`.

(b) Follow the instructions in the installation wizard.

Then carry out the following steps to configure an IP address for your device:

(1) Start the **Dime Manager** from the Windows Start menu: **Start** -> **Programs** -> **funkwerk** -> **Dime Manager**.
The following dialog box appears:

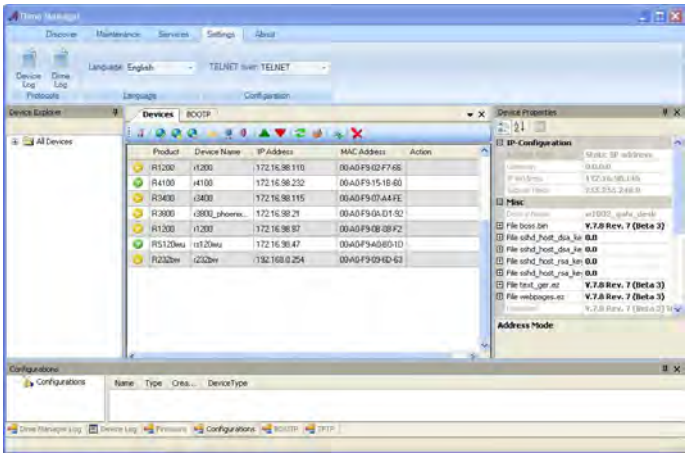


Fig. 7: **Dime Manager** *initial screen*

The **Dime Manager** detects the devices installed in the network.

(2) In the list, double click the device you want to configure.
The following dialog box appears:

Fig. 8: IP address assignment with the **Dime Manager**

(3) Enter the network parameters (**Device name**, **IP address**, **Netmask** and **Gateway**) and click on **OK**.

Note

The maximum length of the **Device name** parameter is 32 characters.

The **Device name** parameter may contain only the letters "a"-"z", "A"-"Z", the digitss "0"-"9", dash "-" and dot "." to avoid errors by other systems during interpretation of the **Device name**. The first character must be a letter, and the last character cannot be a dot "." or dash "-". A single character is not permitted as a name.

Your device can now be reached over the Ethernet with its IP address using a Web browser and can now be configured.

Funkwerk Configuration Interface Call up

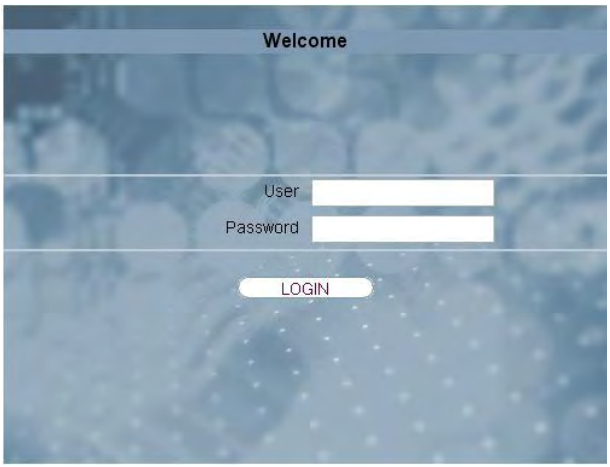


Fig. 9: **Funkwerk Configuration Interface** *Login*

Start the configuration interface as follows:

(a) Enter the IP address of your device in the address line of your Web browser.

With DHCP server:

- the IP address that the DHCP server assigned to your device

Without DHCP server:

- With direct connection to the configuration PC: the fallback IP address *192.168.0.252*
- The fixed IP address assigned via the **Dime Manager**

Press the **Enter (Return) key**.

(b) Enter *admin* in the **User** field and *funkwerk* in the **Password** field.

4.5 Modify system password

All **bintec** devices are delivered with the same username and password. As long as the password remains unchanged, they are therefore not protected against unauthorised use. Make sure you change the passwords to prevent unauthorised access to your device!

Proceed as follows:

(a) Go to **System Management** -> **Global Settings**-> **Passwords**

(b) Enter a new password under **System Admin Password** .

(c) Enter the new password again under **Confirm Admin Password** .

(d) Click **OK**.

(e) Save the configuration by clicking on the **Save Configuration** button above the menu navigation.

Note the following rules on password use:

- The password must not be easy to guess. Names, car registration numbers, dates of birth, etc. should not be chosen as passwords.
- The password should contain at least one character that is not a letter (special character or number).
- The password should be at least 8 characters long.
- Change your password regularly, e.g. every 90 days.

4.6 Setting up a wireless network

If you run your device in Access Point mode, you must set up a wireless network.

Proceed as follows:

(1) Go to **Wireless LAN** -> **WLAN** -> **Wireless Module Settings** -> .

(2) In **Operating Mode**, select *Access Point*.

(3) Leave the default settings in all other fields.

(4) Click **OK**.

(5) Go to **Wireless LAN** -> **WLAN** -> **Wireless Networks (VSS)** -> .

(6) In **Network name (SSID)** enter, for example, *Funkwerk-ec*.

(7) Under **Security Mode**, select *WPA-PSK*.

(8) In **Preshared Key** enter, for example, *supersecret*.

(9) Leave the default settings for all other fields.

(10) Click **OK**.

(11) Save the configuration by clicking on the **Save Configuration** button above the menu navigation.

4.7 Setting up a bridge link

If you run your device in Bridge mode, you must set up a bridge link.

Bridge link autoconfiguration

(1) Go to **Wireless LAN** -> **WLAN** -> **Wireless Module Settings** -> .

(2) In **Operation Mode**, select *Bridge*.

(3) Leave the default settings in all other fields.

(4) Click **OK**.

(5) Go to **Wireless LAN** -> **WLAN** -> **Bridge Links** -> **New**.

(6) In **Preshared Key** enter, for example, *bridgesecret*.

(7) Leave the default settings in all other fields.

(8) Click **OK**.

(9) Configure a bridge link on the remote device in the same way.

(10) For your local device, click the icon in the list in **Wireless LAN** -> **WLAN** -> **Bridge Links** .

(11) In the menu that opens, **Wireless LAN** -> **WLAN** -> **Bridge Links** -> under **Action**, click the *[Scan]* link.

(12) After the scan, the results are listed. For the desired list entry, click on the *[Connect]* link.

(13) Save the configuration by clicking on the **Save Configuration** button above the menu navigation.

To use the bridge link autoconfiguration function, proceed as described in the **Automatic Configuration of a Bridge Link** workshop and read the **Wireless LAN** chapter of the user's guide under **WLAN** -> **Bridge Links** -> **Add**.

Manual configuration

(1) Go to **Wireless LAN** -> **WLAN** -> **Wireless Module Settings** -> **Edit**.

(2) In **Operation Mode**, select *Bridge*.

(3) Leave the default settings in all other fields.

(4) Click **OK**.

(5) Go to **Wireless LAN** -> **WLAN** -> **Bridge Links** ->.

(6) In **Preshared Key** enter, for example, *bridgesecret*.

(7) For **Remote MAC address**, enter the MAC address of the bridge to which your bridge is to set up a connection, e.g. *00:a0:f9:5a:42:53*.

(8) Leave the default settings in all other fields.

(9) Click **OK**.

(10) Configure a bridge link on the remote device in the same way.

(11) Save the configuration by clicking on the **Save Configuration** button above the menu navigation.

Your device is ready for operation when you have completed the configuration.

The configuration of the device and its integration into your network are now completed.

4.8 Software Update

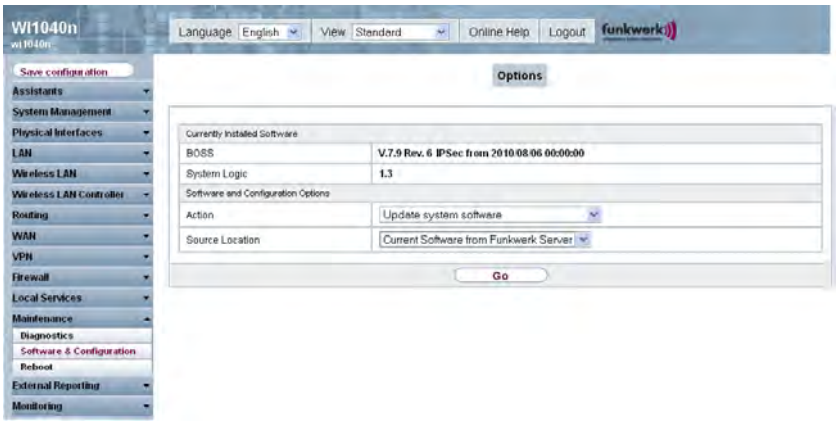
The range of functions of **bintec** devices is continuously being extended. These extensions are made available to you by Funkwerk Enterprise Communications GmbH free of charge. Checking for new software versions and the installation of updates can be carried out easily with the **Funkwerk Configuration Interface**. An existing internet connection is needed for an automatic update.

Proceed as follows:

(1) In the **Maintenance** ->**menu, select Software & Configuration**.

(2) Under **Action**, select *Update System Software* and, under **Source**, *Latest Software from Funkwerk Server.*

(3) Then click on **GO**.



The device will now connect to the Funkwerk Enterprise Communications GmbH download server and check whether an updated version of the system software is available. If so,

your device will be updated automatically. When installation of the new software is complete, you will be invited to restart the device.

Caution

Once you have clicked on **GO** , the update cannot be cancelled/interrupted. If an error occurs during the update, do not re-start the device and contact support.

Chapter 5 Reset

If the configuration is incorrect or if your device cannot be accessed, you can reset the device to the ex works standard settings using the Reset button on the bottom of the device.

Practically al existing configuration data will then be ignored, only the current user passwords are retained. Configurations stored in the device are not deleted and can, if required, be reloaded when the device is rebooted.

For **bintec W1002n** proceed as follows:

(1) Switch off your device.

(2) Press the **Reset** button on your device.

(3) Keep the **Reset** button on your device pressed down and switch the device back on.

(4) Look at the LEDs:
- Initially all LEDs illuminate.
- The device runs through the boot sequence.
- After the LED has flashed three times, release the **Reset** button.
- The *Status* LED flashes and the *Eth 1* and *Eth 2* LEDs illuminate if these exist for the ports that are connected to the Ethernet.

On devices of the **WI series**, the red *Failure* LED flashes first. Hold in the **Cfg** button until the red LED goes out and the green *Status* LED starts to flash.

Proceed as follows if you also want to reset all the user passwords to the ex works state and delete stored configurations when resetting the device:

(1) Set up a serial connection to your device. Reboot your device and monitor the boot sequence. Start the BOOTmonitor (as described in *BOOTmonitor* on page 72) and choose the **(4) Delete configuration** and follow the instructions.
or

(2) Set up a serial connection to your device. First carry out the reset procedure described and enter *erase bootconfig* as **Login** at the login prompt in the command line. Leave the password empty and press the Return key. The device runs through the boot sequence again.

You can now configure your device again as described from *Basic configuration* on page 14.

Note

If you delete the boot configuration using the **Funkwerk Configuration Interface**, all passwords will also be reset and the current boot configuration deleted. The next time, the device will boot with the standard ex works settings.

On devices of the **WI series**, there is a further button - the **HW** reset. After pressing briefly once, the device reboots.

Fig. 10: Underside of the **bintec WIx040n** *with the HW and Cfg reset buttons*

Chapter 6 Technical data

This chapter summarises all of the hardware properties of the devices **W1002n**, **WI1040n**, **WI2040n**, **WI1065n** and **WI2065n**.

Caution

bintec WIx065n is a class A set-up. This set-up can cause interference in living areas; in this case the operator can request for appropriate measures to be taken.

6.1 Scope of supply

Your device is supplied with the following parts:

	Cable sets/mains unit/other	Software	Documentation
bintec W1002n	Ethernet cable (RJ-45, STP) Plug-in power pack (12 V/230 V) 3 external standard antennas Self-adhesive feet to allow the device to be used as a desktop device 2 screws and 2 raw plug for fastening to the wall	Companion DVD	Quick Install Guide (printed) R&TTE Compliance Information (printed) User's Guide (on DVD) Safety notices
bintec WI1040n	Ethernet cable (RJ-45, STP) Serial cable (D-SUB9) 3 external standard antennas Self-adhesive feet to allow the device to be used as a desktop device Blind stops for SFP SD slot cover with screw 3-pole screw terminal bar for the power supply	Companion DVD	Quick Install Guide (printed) R&TTE Compliance Information (printed) User's Guide (on DVD) Safety notices

	Cable sets/mains unit/other	Software	Documentation
	2-pole screw terminal bar for relay Mounting bracket for wall mounting 1 screw pin set Blind stops for Ethernet interfaces		
bintec WI2040n	Ethernet cable (RJ-45, STP) Serial cable (D-SUB9) 4 external standard antennas Self-adhesive feet to allow the device to be used as a desktop device Blind stops for SFP SD slot cover with screw 3-pole screw terminal bar for the power supply 2-pole screw terminal bar for relay Mounting bracket for wall mounting 1 screw pin set Blind stops for Ethernet interfaces	Companion DVD	Quick Install Guide (printed) R&TTE Compliance Information (printed) User's Guide (on DVD) Safety notices
bintec WI1065n	Ethernet cable (RJ-45, STP) Serial cable (D-SUB9) 3 external standard antennas Blind stops for SFP SD slot cover with screw 3-pole screw terminal bar for the power supply 2-pole screw terminal bar for	Companion DVD	Quick Install Guide (printed) R&TTE Compliance Information (printed) User's Guide (on DVD) Safety notices

	Cable sets/mains unit/other	Software	Documentation
	relay 1 screw pin set Blind stops for Ethernet interfaces 4 threaded caps for antennas		
bintec WI2065n	Ethernet cable (RJ-45, STP) Serial cable (D-SUB9) 4 external standard antennas Blind stops for SFP SD slot cover with screw 3-pole screw terminal bar for the power supply 2-pole screw terminal bar for relay 1 screw pin set Blind stops for Ethernet interfaces 4 threaded caps for antennas One set of rubber seals for cable bushings	Companion DVD	Quick Install Guide (printed) R&TTE Compliance Information (printed) User's Guide (on DVD) Safety notices

6.2 General Product Features

The general product features cover performance features and the technical prerequisites for installation and operation of your device.

The features are summarised in the following table:

General Product Features bintec W1002n

Property	Value
bintec W1002n	One internal wireless module, 3 external antennas
Dimensions and weights:	
Equipment dimensions without cable	163 mm x 168 mm x 50 mm

Property	Value
(W x L x H)	
Weight	approx. 430 g
LEDs	4 (1x Status, 1x WLAN, 2x Ethernet)
Power consumption of the device	5-10 Watt, depending on extensions
Voltage supply	External switched-mode power supply 12 V DC, 1.25 A PoE on Ethernet 1 Class 0 (insulated) with one WLAN module
Environmental requirements:	
Storage temperature	-10° to +70 °C
Operating temperature	0° to 40 °C
Relative atmospheric humidity	10 % to 95 % (non-condensing)
Room classification	Only use in dry rooms.
Available interfaces:	
Serial interface V.24	Permanently installed, supports Baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
Ethernet IEEE 802.3 LAN (2-port switch)	Permanently installed (twisted pair only), 10/100 mbps, autosensing, MDIX
Available sockets:	
Serial interface V.24	9-pin Sub-D connector
Ethernet interface	RJ45 socket
Antennas:	
Antenna connection	RTNC socket
Transmit Power	max. 100 mW (20 dBm) EIRP
Receiver sensitivity	2,4 GHz 802.11b/g: 1 Mbit/s -91 dBm; 2 Mbit/s -90 dBm; 5.5 Mbit/s -89 dBm; 11 Mbit/s -88 dBm; 6 Mbit/s -90 dBm;9 Mbit/s -89 dBm; 12 Mbit/s -88 dBm; 18 Mbit/s -86 dBm; 24 Mbit/s -83 dBm; 36 Mbit/s -80 dBm; 48 Mbit/s -76 dBm; 54 Mbit/s -74 dBm 2,4 GHz 802.11n 20 MHz: MSC0 -89 dBm; MSC1 -87 dBm; MCS2 -85 dBm; MCS3 -82 dBm; MCS4 -79 dBm; MSC5 -75 dBm; MCS6 -73 dBm; MCS7 -70 dBm; MCS8 -87 dBm; MCS9 -84 dBm; MCS10 -81 dBm; MCS11 -79 dBm; MCS12 -77 dBm; MCS13 -72 dBm; MCS14 -68 dBm; MCS15 -67 dBm

Property	Value
	2,4 GHz 802.11n 40 MHz: MSC0 -87 dBm; MSC1 -84 dBm; MCS2 -82 dBm; MCS3 -79 dBm; MCS4 -75 dBm; MSC5 -71 dBm; MCS6 -69 dBm; MCS7 -67 dBm; MCS8 -86 dBm; MCS9 -83 dBm; MCS10 -79 dBm; MCS11 -77 dBm; MCS12 -74 dBm; MCS13 -69 dBm; MCS14 -67 dBm; MCS15 -65 dBm 5 GHz 802.11a/h: 6 Mbit/s -88 dBm; 9 Mbit/s -87 dBm; 12 Mbit/s -86 dBm; 18 Mbit/s -84 dBm; 24 Mbit/s -82 dBm; 36 Mbit/s -78 dBm; 48 Mbit/s -74 dBm; 54 Mbit/s -73 dBm; 5 GHz 802.11n 20 MHz: MSC0 -88 dBm; MSC1 -85 dBm; MCS2 -83 dBm; MCS3 -81 dBm; MCS4 -78 dBm; MSC5 -74 dBm; MCS6 -72 dBm; MCS7 -70 dBm; MCS8 -88 dBm; MCS9 -85 dBm; MCS10 -83 dBm; MCS11 -80 dBm; MCS12 -77 dBm; MCS13 -72 dBm; MCS14 -70 dBm; MCS15 -68 dBm 2,4 GHz 802.11n 40 MHz: MSC0 -84 dBm; MSC1 -82 dBm; MCS2 -79 dBm; MCS3 -77 dBm; MCS4 -74 dBm; MSC5 -69 dBm; MCS6 -67 dBm; MCS7 -66 dBm; MCS8 -83 dBm; MCS9 -82 dBm; MCS10 -79 dBm; MCS11 -76 dBm; MCS12 -72 dBm; MCS13 -68 dBm; MCS14 -66 dBm; MCS15 -64 dBm
Modulation	Modulation IEEE 802.11 standards: a,h (5 GHz) b/g (2.4 GHz) Modulation types: 11, 5.5, 2 and 1 Mbit/s (DSSS) 2.4 GHz; 54, 48, 36, 24, 18, 12, 9 and 6 Mbit/s (OFDM) 2.4 and 5 GHz
Channels	IEEE 802.11b/g: 13 channels (Europe) IEEE 802.11a/h: 19 channels (Europe)
Standards	IEEE 802.11a,b,g,d,h,i IEEE 802.11n (MIMO 2T3R) IEEE 802.3 IEEE 802.3af IEEE 802.1q (VLAN Tagging)

Property	Value
Frequency bands	2.4 GHz Indoor/Outdoor (2412-2472 MHz) 5 GHz Indoor (5150-5350 MHz) 5 GHz Outdoor (5470-5725 MHz) 5 GHz BFWA (5755-5875 MHz) only in Germany and Great Britain (reporting obligations in Germany, licencing obligations in Great Britain).
Standards & Guidelines	R&TTE Directive 1999/5/EC EN 60950-1 (IEC60950); EN 300 328; EN 301 489-17;EN 301 489-1; EN 301 893; EN 60601-1-2 (Medical electrical equipment - Part 1-2)
Buttons	A monitor button
Security features	WEP64 (40 bit key), WEP128 (104 bit key), WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise Access Control List, Network Name Broadcast can be deactivated
WEP key length (bit)	40 (64) or 104 (128)
Software supplied	Dime Manager on DVD
Printed documentation supplied	Quick Install Guide Safety notices R&TTE Compliance Information
Online documentation	User's Guide Workshops Release Notes, if applicable

General Product Features bintec WI1040n and bintec WI2040n

Property	Value
Variants:	
bintec WI1040n	An internal wireless module, 3 external antenna (WLAN 1 Ant.1, WLAN 1 Ant.2, WLAN 1 Ant.3)
bintec WI2040n	Two internal wireless modules, 4 external antenna (WLAN 1 Ant.1, WLAN 1 Ant.2, WLAN 2 Ant.1, WLAN 2 Ant.2)

Property	Value
Dimensions and weights:	
Equipment dimensions without cable (W x L x H)	220 mm x 185 mm x 42 mm without feet
Weight	approx. 1,200 g (3 WLAN modules)
LEDs	**bintec WI1040n** 6 (1x Failure, 1x Status, 3x WLAN, 2x Ethernet, 1x SFP) **bintec WI2040n** 7 (1x Failure, 1x Status, 3x WLAN, 2x Ethernet, 1x SFP)
Power consumption of the device	5-24 Watt, depending on extensions
Voltage supply	Earth conductor/connection to earth 5-20W. All devices must be earthed. 24 V ± 30 % DC 1,1 A with reverse voltage protection, insulated 3-pole PoE on Ethernet 1 Class 0 (insulated) with max. two WLAN modules
Protection against theft	Theft protection is available as an option
Temperature sensor	Temperature monitoring and software-controlled actions possible
Environmental requirements:	
Storage temperature	-40 °C to +85 °C
Operating temperature	-25 °C to +70 °C
Relative atmospheric humidity	10 % to 95 % (non-condensing)
Room classification	Operate only in dry rooms
Available interfaces:	
Serial interface V.24	Permanently installed, supports Baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
Ethernet IEEE 802.3 LAN	Permanently installed (twisted pair only), 10/100 mbps, autosensing, MDI/MDIX 2x 10/100 Base T/TX
Relay	An alarm using relay is possible in the event of overtemperature or error: potential-free working contact, 42 V AC 1 A / 30 V DC 2 A
Optical interface	Module slot for optical interface 100 mbps LWL Single Mode LC or LWL Multimode LC - 1x 100 Base FX/SX with SFP module
Available sockets:	

Property	Value
Serial interface V.24	9-pin Sub-D connector
Relay switching contact N/O	42 V AC 1 A / 30 V DC 2 A potential-free, software configurable, switchable
Ethernet interface	RJ45 socket
Antennas:	
Antenna connection	RTNC socket
Transmit Power (WLAN)	max. 100 mW (20 dBm) EIRP
Receiver sensitivity	5 GHz 802.11a/h: 6 Mbit/s -88 dBm;9 Mbit/s -87 dBm; 12 Mbit/s -86 dBm; 18 Mbit/s -84 dBm; 24 Mbit/s -82 dBm; 36 Mbit/s -78 dBm; 48 Mbit/s -74 dBm; 54 Mbit/s -73 dBm; 2,4 GHz 802.11b/g: 1 Mbit/s -91 dBm; 2 Mbit/s -90 dBm; 5.5 Mbit/s -89 dBm; 11 Mbit/s -88 dBm; 6 Mbit/s -90 dBm;9 Mbit/s -89 dBm; 12 Mbit/s -88 dBm; 18 Mbit/s -86 dBm; 24 Mbit/s -83 dBm; 36 Mbit/s -80 dBm; 48 Mbit/s -76 dBm; 54 Mbit/s -74 dBm
Modulation	Modulation IEEE 802.11 standards: a,h (5 GHz) b/g (2.4 GHz) Modulation types: 11, 5.5, 2 and 1 Mbit/s (DSSS) 2.4 GHz; 54, 48, 36, 24, 18, 12, 9 and 6 Mbit/s (OFDM) 2.4 and 5 GHz
Channels	IEEE802.11b/g: 13 channels (Europe) IEEE802.11a/h: 19 channels (Europe)
Standards	IEEE 802.11a,b,g,d,h,i IEEE 802.3 IEEE 802.3af IEEE 802.1q (VLAN Tagging)
Standards & Guidelines	R&TTE Directive 1999/5/EC EN 60950-1 (IEC60950); EN 60950-22; EN 301489-1; EN301489-17; EN 55022; EN 300328-1; EN 301893; EN 302502; EN 50371 (Medical equipment EN 60601-1; EN 60601-2; EN 55011)

Property	Value
	E1-mark (vehicle licencing)
Buttons	Reset and reset to ex work settings possible with two buttons (1x config reset, 1x HW reset)
Security features	WEP, WPA, WPA2, Access Control List, Network Name Broadcast can be deactivated
WEP key length (bit)	40 (64) or 104 (128)
Software supplied	Dime Manager on DVD
Printed documentation supplied	Quick Install Guide Safety notices R&TTE Compliance Information
Online documentation	User's Guide Workshops Release Notes, if applicable

General Product Features bintec WI1065n and bintec WI2065n

Property	Value
Variants:	
bintec WI1065n	An internal wireless module, 3 external antenna (WLAN 1 Ant.1, WLAN 1 Ant.2, WLAN 1 Ant.3)
bintec WI2065n	Two internal wireless modules, 4 external antenna (WLAN 1 Ant.1, WLAN 1 Ant.2, WLAN 2 Ant.1, WLAN 2 Ant.2)
Dimensions and weights:	
Equipment dimensions without cable (W x L x H)	257 mm x 285 mm x 60 mm
Weight	approx. 1900 g (3 WLAN modules)
LEDs	8 (1x Failure, 1x Status, 3x WLAN, 2x Ethernet, 1x SFP)
Power consumption of the device	5-24 Watt, depending on extensions
Voltage supply	Earth conductor/connection to earth 5-20W. All devices must be earthed. 24 V ± 30% DC 1,1 A with reverse voltage protection, insulated 3-pole PoE on Ethernet 1 Class 0 (insulated) with max. two

Property	Value
	WLAN modules
Protection against theft	Theft protection is available as an option
Temperature sensor	Temperature monitoring and software-controlled actions possible
Environmental requirements:	
Storage temperature	-40 °C to +85 °C
Operating temperature	-20 °C to +65 °C
Relative atmospheric humidity	10 % to 100 %
Available interfaces:	
Serial interface V.24	Permanently installed, supports Baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
Ethernet IEEE 802.3 LAN	Permanently installed (twisted pair only), 10/100 mbps, autosensing, MDI/MDIX 2x 10/100 Base T/TX
Relay	An alarm using relay is possible in the event of overtemperature or error: potential-free working contact, 42 V AC 1 A / 30 V DC 2 A
Optical interface	Module slot for optical interface 100 mbps LWL Single Mode LC or LWL Multimode LC - 1x 100 Base FX/SX with SFP module
Available sockets:	
Serial interface V.24	9-pin Sub-D connector
Relay switching contact N/O	42 V AC 1 A / 30 V DC 2 A potential-free, software configurable, switchable
Ethernet interface	RJ45 socket
Antennas:	
Antenna connection	RTNC socket
Transmit Power (WLAN)	max. 100 mW (20 dBm) EIRP
Receiver sensitivity	5 GHz 802.11a/h: 6 Mbit/s -88 dBm;9 Mbit/s -87 dBm; 12 Mbit/s -86 dBm; 18 Mbit/s -84 dBm; 24 Mbit/s -82 dBm; 36 Mbit/s -78 dBm; 48 Mbit/s -74 dBm; 54 Mbit/s -73 dBm; 2,4 GHz 802.11b/g: 1 Mbit/s -91 dBm; 2 Mbit/s -90 dBm; 5.5 Mbit/s -89 dBm; 11 Mbit/s -88 dBm; 6 Mbit/s -90 dBm;9 Mbit/s -89 dBm; 12 Mbit/s -88 dBm; 18 Mbit/s -86 dBm; 24 Mbit/s -83 dBm; 36 Mbit/s -80 dBm; 48 Mbit/s -76 dBm; 54 Mbit/s -74 dBm

Property	Value
Modulation	Modulation IEEE 802.11 standards: a,h (5 GHz) b/g (2.4 GHz) Modulation types: 11, 5.5, 2 and 1 Mbit/s (DSSS) 2.4 GHz; 54, 48, 36, 24, 18, 12, 9 and 6 Mbit/s (OFDM) 2.4 and 5 GHz
Channels	IEEE802.11b/g: 13 channels (Europe) IEEE802.11a/h: 19 channels (Europe)
Standards	IEEE 802.11a,b,g,d,h,i IEEE 802.3 IEEE 802.3af IEEE 802.1q (VLAN Tagging)
Standards & Guidelines	R&TTE Directive 1999/5/EC EN 60950-1 (IEC60950); EN 60950-22; EN 301489-1; EN301489-17; EN 55022; EN 300328-1; EN 301893; EN 302502; EN 50371
Buttons	Reset and reset to ex work settings possible with two buttons (1x config reset, 1x HW reset)
Security features	WEP, WPA, WPA2, Access Control List, Network Name Broadcast can be deactivated
WEP key length (bit)	40 (64) or 104 (128)
Software supplied	Dime Manager on DVD
Printed documentation supplied	Quick Install Guide Safety notices R&TTE Compliance Information
Online documentation	User's Guide Workshops Release Notes, if applicable

To ensure safe operation, the WI series devices have a connection to earth. The minimum cross-section of the earth lead should be 1.5 mm². The distance between the device and the connection to earth should be as short as possible. For the **bintec WIx065n** devices,

the connection to earth is under the cover.

Fig. 11: Connection to earth **bintec WIx040n**

6.3 LEDs

The LEDs show the radio status, radio activity, Ethernet activity and LED states of your device. The LED states are indicated by combinations of the LEDs which are explained in detail in this chapter.

The LEDs on **bintec W1002n** are arranged as follows:

Fig. 12: LEDs of **bintec W1002n**

In operation mode, the LEDs display the following status information for your device:

LED status display bintec W1002n

LED	Status	Information
Status	off	The power supply is not connected. If other LEDs are on, also Error.
	on (static)	Errors
	on (flashing)	Ready
WLAN (1/2)	on (flashing slowly)	Free
	on (static)	At least one client is registered.
	on (flickering)	At least one client is registered and there is data traffic.
	on (flashing fast)	BLD (Broken Link Detection) active
	on (flashing fast)	5 GHz scan active

LED	Status	Information
ETH 1/2	off	No cable or no Ethernet link
	on	Cable plugged in and link
	on (flickering)	Cable plugged in and link with data traffic

During the heating phase the red Failure LED flashes. Once this temperature has been reached, the device continues with the start-up process.

All LEDs are on during the start-up process. This means the monitor has been started and firmware is being loaded.

Note

Note that the number of active WLAN LEDs depends on the number of existing wireless modules.

The LEDs on **bintec WI1040n** and **bintec WI2040n** are arranged as follows:

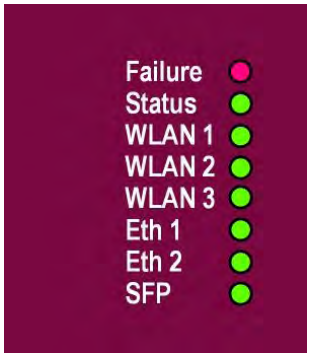


Fig. 13: LEDs of **bintec WI1040n** *and* **bintec WI2040n**

In operation mode, the LEDs display the following status information for your device:

LED status display bintec WI1040n and bintec WI2040n

LED	Status	Information
Failure (red)	on	After power-up and during booting or if an error occurs.
	flashes	During the heating phase.
	off	If the device is at the login prompt.
Status (green)	off	The power supply is not connected. If other LEDs are on, also Error.

LED	Status	Information
	on (static)	Errors
	on (flashing)	Ready
WLAN 1/2/3 (3x green)	on (flashing slowly)	Free
	on (static)	At least one client is registered.
	on (flickering)	At least one client is registered and there is data traffic.
	on (flashing fast)	BLD (Broken Link Detection) active
	on (flashing fast)	5 GHz scan active
ETH 1/2 (2x green)	off	No cable or no Ethernet link
	on	Cable plugged in and link
	on (flickering)	Cable plugged in and link with data traffic
SFP (green)	off	No data traffic
	on	Data traffic via the SFP interface.
	on (flickering)	Cable plugged in and data traffic

During the heating phase the red Failure LED flashes. The other LEDs then come on during booting (if the units are initialised).

Note

Note that the number of active WLAN LEDs depends on the number of existing wireless modules.

The LEDs on **bintec WI1065n** and **bintec WI2065n** are arranged as follows:

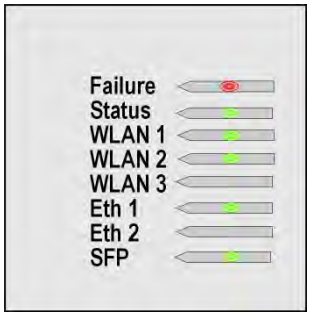


Fig. 14: LEDs of **bintec WI1065n** *and* **bintec WI2065n**

In operation mode, the LEDs display the following status information for your device:

LED status display bintec WI1065n and bintec WI2065n

LED	Status	Information
Failure (red)	on	After power-up and during booting or if an error occurs.
	flashes	During the heating phase.
	off	If the device is at the login prompt.
Status (green)	off	The power supply is not connected. If other LEDs are on, also Error.
	on (static)	Errors
	on (flashing)	Ready
WLAN 1/2/3 (3x green)	on (flashing slowly)	Free
	on (static)	At least one client is registered
	on (flickering)	At least one client is registered and there is data traffic
	on (flashing fast)	BLD (Broken Link Detection) active
	on (flashing fast)	5 GHz scan active
ETH 1/2 (2x green)	off	No cable or no Ethernet link
	on	Cable plugged in and link
	on (flickering)	Cable plugged in and link with data traffic
SFP (green)	off	No data traffic
	on	Data traffic via the SFP interface.
	on (flickering)	Cable plugged in and data traffic

During the boot operation, only the red LED is on. The other LEDs then come on during booting (if the units are initialised).

6.4 Connectors

All the connections are located on the underside of the device.

On **bintec W1002n** the third antenna connection is located on the underside of the device.

The connectors on industrial WLAN devices with 802.11n support are the same as the connectors on other industrial WLAN devices. Only the assignment of the antenna connectors is different. See *Antenna connectors for industrial WLAN devices with 802.11n support* on page 45.

bintec W1002n has two Ethernet connections and a serial interface.

The connections are arranged as follows:

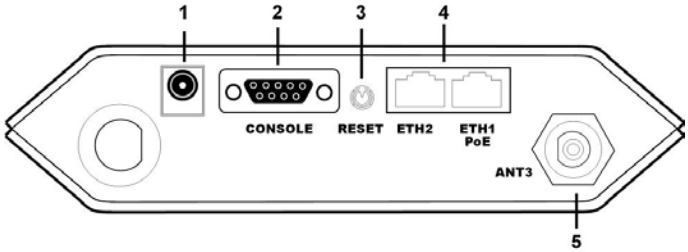


Fig. 15: **bintec W1002n** *underside*

bintec W1002n underside

1	POWER	Socket for plug-in power pack
2	CONSOLE	Serial interface
3	RESET	Reset button
4	ETH1/PoE and ETH2	10/100 Base-T Ethernet interface
5	ANT3	Connections for screwing on the external antennas ANT3 = RX3
Top without Fig.	ANT1/ANT2	Connections for screwing on the external antennas ANT1 = TX/RX1 (Connection of first directional antenna)

		ANT2 = TX/RX2 (Connection of second option directional antenna)

bintec WI1040n, and **bintec WI2040n** have two Ethernet connections and a serial interface.

The connections are arranged as follows:

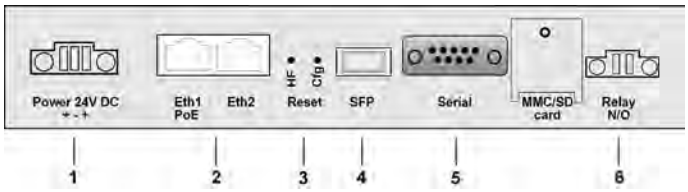


Fig. 16: Underside **bintec WI1040n** *and* **bintec WI2040n**

Underside of bintec WI1040n and bintec WI2040n

1	Power 24V DC	Socket for power supply
2	Eth1 (PoE) / Eth2	10/100 Base-T Ethernet interfaces
3	Reset (HW and Cfg)	Reset button and delete configuration
4	SFP	SFP slot for 100 Mbit/s fibre module (optional)
5	Serial	Serial interface RS232
6	Relay N/O	Alarm relay

bintec WI1065n and **bintec WI2065n** have two Ethernet connections and a serial interface.

The connections are arranged as follows:

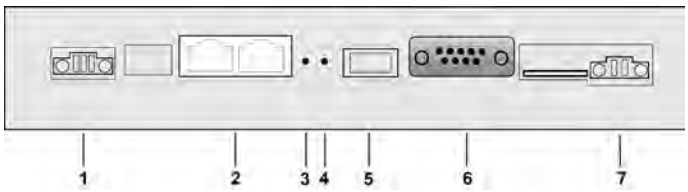


Fig. 17: Underside **bintec WI1065n** *and* **bintec WI2065n**

Underside of bintec WI1065n and bintec WI2065n

1	Power 24 V DC	Socket for power supply
2	Eth1 PoE / Eth2	10/100 Base-T Ethernet interfaces

3	HW	Reset button performs restart
4	Cfg	Deletes the configuration
5	SFP	SFP slot for 100 Mbit/s fibre module (optional)
6	Serial	Serial interface RS232
7	Relay N/O	Alarm relay contact

6.5 Antenna connectors for industrial WLAN devices with 802.11n support

Note

The three antenna for devices **bintec WI1040n**, **bintec WI1065n** and **bintec W1002n** have 2 Transmit and 3 Receive functions in n operating mode MIMO 2T3R. WLAN 1 Ant. 1 and WLAN 1 Ant. send and receive, Ant. 3 only receives.

For devices **bintec WI2040n** and **bintec WI2065n** only 2 antenna are used for each of the 2 wireless modules. These are both sending and receiving antenna. There is no third receiving antenna; this is MIMO 2T2R operating mode.

However gross rates of 300 Mbps are possible. The receiving sensitivity decreases slightly. Only 2 antenna connections are required to operate bridgelink with dual polarisation antenna.

Antenna should be Lambda/2 or a multiple of this. In **bintec WIx040n** the antenna are 37 mm apart; in **bintec WIx065n** the antenna are 55 mm apart.

2.4 GHz Lambda/2 corresponds to 6.15 cm; 5 GHz Lambda/2 corresponds to 2.72 cm.

Devices with 802.11n support can use up to 3 antenna per wireless module. The assignment of the existing 4 antenna connectors is shown in the following graphic:

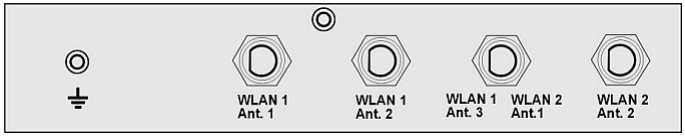


Fig. 18: Antenna configuration for **bintec WIx040n** *devices*

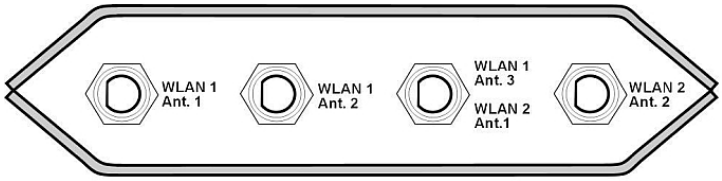


Fig. 19: Antenna configuration for **bintec WIx065n** *devices*

6.6 Pin Assignments

6.6.1 Ethernet interface

Your device has two Ethernet interfaces. These are used to connect individual PCs or other switches.

The connection is made via an RJ45 socket.

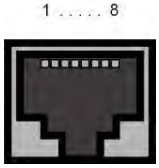


Fig. 20: Ethernet 10/100 Base-T interface (RJ45 socket)

The pin assignment for the Ethernet 10/100 Base-T interface (RJ45 socket) is as follows:

RJ45 socket for LAN connection

Pin	Function Eth1 - PoE	Function Eth 2
1	TD +/Power	TD +
2	TD -/Power	TD -
3	RD +/Power	RD +
4	Power	Not used
5	Power	Not used
6	RD -/Power	RD -
7	Power	Not used
8	Power	Not used

The Ethernet 10/100 BASE-T interface does not have an Auto-MDI-X function in **bintec**

W1002n.

6.6.2 Serial interface

Your device has a Serial interface for connection to a console. This supports Baud rates from 1200 to 115200 Bps.

The interface is designed as a 9-pin SUB-D socket.

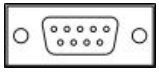


Fig. 21: 9-pin Sub-D connector

The pin assignment is as follows:

Pin assignment of the Sub-D port

Pin	bintec W1002n function
1	Not used
2	RxD
3	TxD
4	Not used
5	GND
6	DSR
7	RTS
8	CTS
9	Not used

6.6.3 Socket for power supply

The WI devices have a 3-pole connection for the power supply. An individual power supply can be connected with any polarity and to any terminal with 2 pins. If a redundant power supply is selected (2 mains units) the minus poles must be connected together to terminal 2 and the plus poles must be connected separately to terminals 1 and 3.

Fig. 22: 3-pole connector for the power supply

The pin assignment is as follows:

Pin assignment of the connector for the power supply

Pin	Configuration
1	+
2	-
3	+

6.7 Frequencies and channels

Different certification regulations apply around the world. ETSI standards generally apply (predominantly used in Europe). For operation in Europe, please read the notes in the R&TTE Compliance Information.

6.8 WEEE information

The waste container symbol with the »X« through it on the device indicates that the device must be disposed of separately from normal domestic waste at an appropriate waste disposal facility at the end of its useful service life.

Das auf dem Gerät befindliche Symbol mit dem durchgekreuzten Müllcontainer bedeutet, dass das Gerät am Ende der Nutzungsdauer bei den hierfür vorgesehenen Entsorgungsstellen getrennt vom normalen Hausmüll zu entsorgen ist.

Le symbole se trouvant sur l'appareil et qui représente un conteneur à ordures barré signifie que l'appareil, une fois que sa durée d'utilisation a expiré, doit être éliminé dans des poubelles spéciales prévues à cet effet, de manière séparée des ordures ménagères courantes.

Il simbolo raffigurante il bidone della spazzatura barrato riportato sull'apparecchiatura significa che alla fine della durata in vita dell'apparecchiatura questa dovrà essere smaltita separatamente dai rifiuti domestici nei punti di raccolta previsti a tale scopo.

El símbolo del contenedor con la cruz, que se encuentra en el aparato, significa que cuando el equipo haya llegado al final de su vida útil, deberá ser llevado a los centros de recogida previstos, y que su tratamiento debe estar separado del de los residuos urbanos.

Symbolen som sitter på apparaten med den korsade avfallstunnan betyder att apparaten när den tjänat ut ska kasseras och lämnas till de förutsedda sortergårdarna och skiljas från normalt hushållsavfall.

Tegnet på apparatet som viser en avfallcontainer med et kyss over, betyr at apparatet må kastet på hertil egnet avfallssted og ikke sammen med vanlig avfall fra husholdningen.

Το σύμβολο που βρίσκεται στην συσκευή με το σταυρωμένο κοντέϊνερ απορριμμάτων σημαίνει, ότι η συσκευή στο τέλος της διάρκειας χρήσης της πρέπει να διατεθεί ξεχωριστά από τα κανονικά απορρίμματα στα γι' αυτό τον σκοπό προβλεπόμενα σημεία διάθεσης.

Symbolet med gennemkrydset affaldsbeholder på apparatet betyder, at apparatet, når det ikke kan bruges længere, skal bortskaffes adskilt fra normalt husholdningsaffald på et af de dertil beregnede bortskaffelsessteder.

Znajdujący się na urządzeniu symbol przekreślonego pojemnika na śmieci oznacza, że po upływie żywotności urządzenia należy go oddać do odpowiedniej placówki utylizacyjnej i nie wyrzucać go do normalnych śmieci domowych.

Het doorgehaalde symbool van de afvalcontainer op het apparaat betekent dat het apparaat op het einde van zijn levensduur niet bij het normale huisvuil mag worden verwijderd. Het moet bij een erkend inzamelpunt worden ingeleverd.

O símbolo com um caixote de lixo riscado, que se encontra no aparelho, significa, que o aparelho no fim da sua vida útil deve ser eliminado separadamente do lixo doméstico nos centros de recolha adequados.

Chapter 7 Access and configuration

This chapter describes all the access and configuration options.

7.1 Access Options

The various access options are presented below. Select the procedure to suit your needs.

There are various ways you can access your device to configure it:

- Via your LAN
- Via the serial interface

7.1.1 Access via LAN

Access via one of the Ethernet interfaces of your device allows you to to open the **Funkwerk Configuration Interface** in a web browser for configuration purposes and to access your device via Telnet or SSH.

Caution

If you carry out the initial configuration with the **Funkwerk Configuration Interface**, this can result in inconsistencies or malfunctions, as soon as you carry out additional settings using other configuration options. Therefore, it is recommended that the configuration is continued with the **Funkwerk Configuration Interface**. If you use SNMP shell commands, continue with this configuration method.

7.1.1.1 HTTP/HTTPS

With a current web browser, you can use the HTML interfaces to configure your device.

The configuration can be set up using the **Funkwerk Configuration Interface**. To do this, enter the IP address of your device in the address field of your Web browser.

With DHCP server:

- the IP address that your DHCP server assigned to your device

Without DHCP server:

- With direct connection to the configuration PC: the fallback IP address `192.168.0.252`

- The fixed IP address assigned via the **Dime Manager**

Press the **Enter (Return) key**.

7.1.1.2 Telnet

Apart from configuration using a web browser, with a Telnet connection you can also access the SNMP shell and use other configuration options.

You do not need any additional software on your PC to set up a Telnet connection to your device. Telnet is available on all operating systems.

Proceed as follows:

Windows

(1) Click **Run…** in the Windows Start menu.

(2) Enter `telnet <IP address of your device>`.

(3) Click **OK**.
A window with the login prompt appears. You are now in the SNMP shell of your device.

(4) Continue with *Logging in for Configuration* on page 56.

Unix

You can also set up a Telnet connection on UNIX and Linux without any problem:

(1) Enter `telnet <IP address of your device>` in a terminal.
A window with the login prompt appears. You are now in the SNMP shell of your device.

(2) Continue with *Logging in for Configuration* on page 56.

7.1.1.3 SSH

In addition to the unencrypted and potentially viewable Telnet session, you can also connect to your device via an SSH connection. This is encrypted, so all the remote maintenance options can be carried out securely.

The following preconditions must be met in order to connect to the device via SSH:

- The encryption keys needed for the process must be available on the device.
- An SSH client must be installed on your PC.

Encryption keys

First of all, make sure that the keys for encrypting the connection are available on your

device:

(1) Log in to one of the types already available on your device (e.g. via Telnet - for login see *Logging in* on page 55).

(2) Enter `update -i` for the input prompt. You are now in the Flash Management shell.

(3) Call up a list of all the files saved on the device: `ls -al`.

If you see a display like the one below, the keys needed are already there and you can connect to the device via SSH:

```
Flash-Sh > ls -al

Flags Version Length Date Name ...

Vr-xpbc-B 7.1.04 2994754 2004/09/02 14:11:48 box150_srel.ppc860

Vrw-pl--f 0.0 350 2004/09/07 10:44:14 sshd_host_rsa_key.pub

Vrw-pl--f 0.0 1011 2004/09/07 10:44:12 sshd_host_rsa_key

Vrw-pl--f 0.0.01 730 2004/09/07 10:42:17 sshd_host_dsa_key.pub

Vrw-pl--f 0.0.01 796 2004/09/07 10:42:16 sshd_host_dsa_key

Flash-Sh >
```

Note

The device generates a key pair for each of the algorithms (RSA and DSA), i.e. two files must be stored in the flash for each algorithm (see example at above).

If no keys are available, you have to generate these first. Proceed as follows:

(1) Leave the Flash Management shell with `exit`.

(2) Call up the Setup tool (`setup`) and navigate to the **Security** -> **SSH Daemon** -> **Certification Management** menu.

(3) To have the keys generated by the device, mark one of the two entries with the cursor and confirm with **Enter**. The device then generates the key and stores it in the FlashROM.

(4) Make sure that both keys have been successfully generated. To do this, repeat the procedure described above.

Login via SSH

Proceed as follows to log in on your device via SSH:

If you have made sure that all the keys needed are available on the device, you have to check whether an SSH client is installed on your PC. Most UNIX and Linux distributions install a SSH client by default. Additional software, e.g. PuTTY, usually has to be installed on a Windows PC.

Proceed as follows to log in on your device via SSH:

UNIX

(1) Enter `ssh <IP address of the device>` in a terminal.
The login prompt window appears. This is located in the SNMP shell of the device.

(2) Continue with *Logging in* on page 55.

Windows

(1) How an SSH connection is set up very much depends on the software used. Consult the documentation for the program you are using.
As soon as you have connected to the device, the login prompt window will appear. You are now in the SNMP shell of your gateway.

(2) Continue with *Logging in* on page 55.

Note

PuTTY requires certain settings for a connection to a **bintec** device. The support pages of *http://www.funkwerk-ec.com* include FAQs, which list the required settings.

7.1.2 Access via the Serial Interface

Your device has a serial interface, with which a PC can be connected directly. The following chapter describes what you have to remember when setting up a serial connection and what you can do to configure your device in this way.

Access via the serial interface is ideal if you are setting up an initial configuration of your device and a LAN access is not possible via the pre-configured IP address (192.168.0.252/255.255.255.0).

Windows

To connect your device to your PC via the serial interface, proceed as described in *Installation* **on page 6**.

If you are using a Windows PC, you need a terminal program for the serial connection, e.g. HyperTerminal. Make sure that HyperTerminal was also installed on the PC with the Windows installation. However, you can also use any other terminal program that can be set to

the corresponding parameters (see below).

Proceed as follows to access your device via the serial interface:

(1) Click on **Programs** -> **Accessories** -> **HyperTerminal** in the Windows Start menu.

(2) Press **Return** (at least once) after the HyperTerminal window opens.

A window with the login prompt appears. You are now in the SNMP shell of your device. You can now log in on your device and start the configuration.

Check

If the login prompt does not appear after you press **Return** several times, the connection to your device has not been set up successfully.

Therefore, check the COM1 or COM2 settings on your PC.

(1) Click on **File** ->**Properties**.

(2) Click **Configure** in the **Connect to** tab.
The following settings are necessary:
- Bits per second: *9600*
- Data bits: *8*
- Parity: *open*
- Stopbits: *1*
- Flow control: *open*

(3) Enter the values and click **OK**.

(4) Make the following settings in the **Settings** tab:
- Emulation: *VT100*

(5) Click **OK**.

The changes to the terminal program settings do not take effect until you disconnect the connection to your device and then make the connection again.

If you use HyperTerminal, there may be problems with displaying umlauts and other special characters. If necessary, therefore, set HyperTerminal to *Autodetection* instead of *VT 100*.

Unix

You will require a terminal program such as `cu` (on System V), `tip` (on BSD) or `minicom` (on Linux). The settings for these programs correspond to those listed above.

Example of a command line for using `cu`: `cu -s 9600 -c/dev/ttyS1`

Example of a command line for using `tip`: `tip -9600 /dev/ttyS1`

7.2 Logging in

With the help of certain access data, you can log in on your device and carry out different actions. The extent of the actions available depend on the authorisations of the user concerned.

A login prompt appears first, regardless of how you access your device. You cannot view any information on the device or change the configuration without authentication.

7.2.1 User names and passwords in ex works state

In its ex works state, your device is provided with the following user names and passwords:

User names and passwords in ex works state

User Name	Password	Authorisations
`admin`	`funkwerk`	Read and change system variables, save configurations; use **Funkwerk Configuration Interface**.
`write`	`public`	Read and write system variables (except passwords) (changes are lost when you switch off your device).
`read`	`public`	Read system variables (except passwords).

It is only possible to change and save configurations if you log in with the user name `admin`. Access information (user names and passwords) can also only be changed if you log in with the user name `admin`. For security reasons, passwords are normally shown on the Setup Tool screen not in plain text, but only as asterisks. The user names, on the other hand, are displayed as plain text.

The security concept of your device enables you to read all the other configuration settings with the user name `read`, but not the access information. It is therefore impossible to log in with `read`, read the password of the `admin` user and subsequently log in with `admin` and make changes to the configuration.

Caution

All **bintec** devices are delivered with the same username and password. As long as the password remains unchanged, they are therefore not protected against unauthorised use. How to change the passwords is described in on page .

Make sure you change the passwords to prevent unauthorised access to your device!

If you have forgotten your password, you must reset your device to the ex works state, which means your configuration will be lost.

7.2.2 Logging in for Configuration

Set up a connection to the device. The access options are described in *Access Options* on page 50.

Funkwerk Configuration Interface

Log in via the HTML surface as follows:

(1) Enter your user name in the **User** field of the input window.

(2) Enter your password in the **Password** field of the input window and confirm with **Return** or click the **Login** button.

The status page of the **Funkwerk Configuration Interface** opens in the browser.

SNMP shell

Log into the SNMP shell as follows:

(1) Enter your user name e.g. `admin`, and confirm with **Return**.

(2) Enter your user password e.g. `funkwerk`, and confirm with **Return**.

Your device logs in with the input prompt, e.g. `w1002:>`. The login was successful. You are now in the SNMP shell.

To leave the SNMP shell after completing the configuration, enter `exit` and press **Return**.

7.3 Configuration options

This chapter first offers an overview of the various tools you can use for configuration of your device.

You can configure your device in the following ways:

- **Funkwerk Configuration Interface**
- Assistant
- SNMP shell commands

Note

The detailed help system of the Assistant will help you to clarify any questions you may have. Therefore the wizard will not be discussed in any greater detail in this document.

The configuration options available to you depend on the type of connection to your device:

Types of connections and configurations

Type of connection	Possible types of configuration
LAN	Assistant, **Funkwerk Configuration Interface**, shell commands
Serial connection	Shell command

Therefore, several types of configuration are available for each type of connection.

Note

To change the device configuration, you must log in with the user name `admin`. If you do not know the password, you cannot make any configuration settings. This applies to all types of configuration.

7.3.1 Funkwerk Configuration Interface for advanced users

Funkwerk Configuration Interface is a web-based graphic user surface that you can use from any PC with an up-to-date Web browser via an HTTP or HTTPS connection.

With the **Funkwerk Configuration Interface** you can perform all the configuration tasks easily and conveniently. It is integrated in your device and is available in English. If required, other languages can be downloaded from the download area of *www.funkwerk-ec.com* and installed on your device.

The settings you make with the **Funkwerk Configuration Interface** are applied with the **OK** or **Apply** button of the menu, and you do not have to restart the device.

If you finish the configuration and want to save your settings so that they are loaded as the boot configuration when you reboot your device, save these by clicking the **Save configuration** button.

You can also use the **Funkwerk Configuration Interface** to monitor the most important function parameters of your device.

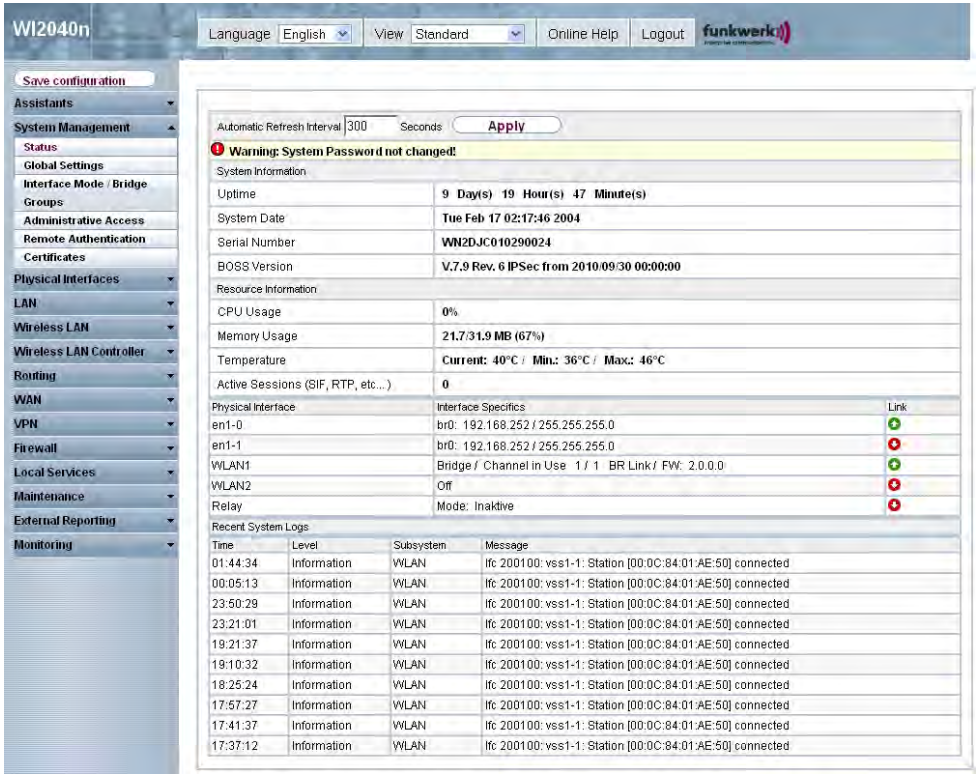

WI2040n
Language English
View Standard
Online Help
Logout
funkwerk
Save configuration
Assistants
System Management
Status
Global Settings
Interface Mode / Bridge Groups
Administrative Access
Remote Authentication
Certificates
Physical Interfaces
LAN
Wireless LAN
Wireless LAN Controller
Routing
WAN
VPN
Firewall
Local Services
Maintenance
External Reporting
Monitoring
Automatic Refresh Interval 300 Seconds Apply
Warning: System Password not changed!
System Information
Uptime 9 Day(s) 19 Hour(s) 47 Minute(s)
System Date Tue Feb 17 02:17:46 2004
Serial Number WN2DJC010290024
BOSS Version V.7.9 Rev. 6 IPSec from 2010/09/30 00:00:00
Resource Information
CPU Usage 0%
Memory Usage 21.7/31.9 MB (67%)
Temperature Current: 40°C / Min.: 36°C / Max.: 46°C
Active Sessions (SIP, RTP, etc...) 0
Physical Interface Interface Specifics Link
en1-0 br0: 192.168.252 / 255.255.255.0
en1-1 br0: 192.168.252 / 255.255.255.0
WLAN1 Bridge / Channel in Use 1 / 1 BR Link / FW: 2.0.0.0
WLAN2 Off
Relay Mode: Inaktive
Recent System Logs
Time Level Subsystem Message
01:44:34 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
00:05:13 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
23:50:29 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
23:21:01 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
19:21:37 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
19:10:32 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
18:25:24 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
17:57:27 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
17:41:37 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
17:37:12 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected

Fig. 24: **Funkwerk Configuration Interface** *home page*

7.3.1.1 Calling up Funkwerk Configuration Interface

(1) Check whether the device is connected and switched on and that all the necessary cables are correctly connected (see *Technical data* on page 28).

(2) Check the settings of the PC from which you want to configure your device (see *Configuring a PC* on page 18).

(3) Open a web browser.

(4) Enter `http://192.168.0.252` (or the IP address dynamically assigned by your DHCP server or the address statically assigned by you with the **Dime Manager**) in the Web browser's address field.

(5) Enter `admin` in the **User** field and `funkwerk` in the **Password** field and click **LOGIN**.

You are not in the status menu of your device's **Funkwerk Configuration Interface** (see *Status* on page 75).

7.3.1.2 Operating elements

Funkwerk Configuration Interface window

The **Funkwerk Configuration Interface** window is divided into three areas:

- The header
- The navigation bar
- The main configuration window

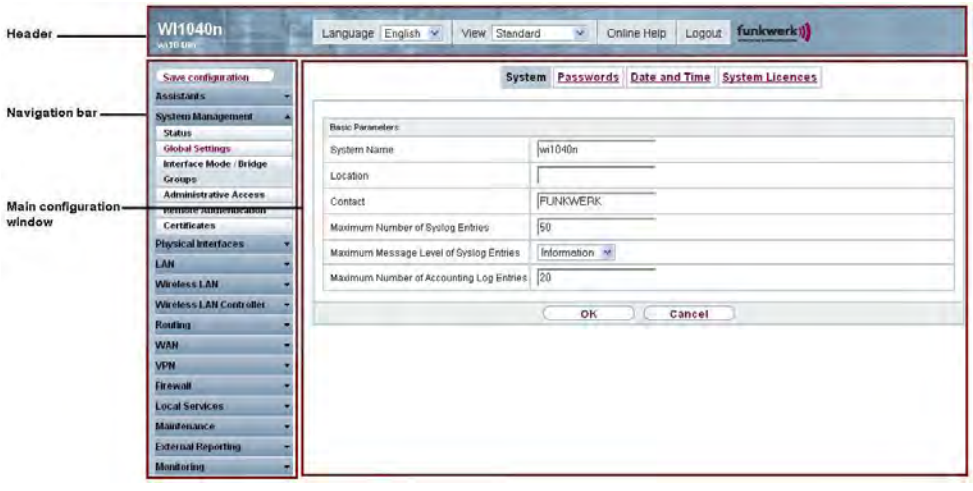


Fig. 25: Areas of the **Funkwerk Configuration Interface**

Header

Fig. 26: **Funkwerk Configuration Interface** *header*

Funkwerk Configuration Interface header

	Function
Language English	**Language selection**: From the dropdown menu, select the language in which the **Funkwerk Configuration Interface** is to be displayed. Here, you can select the language in which you want

	Function
	to carry out the configuration. German and English are available.
View Standard	**View**: Select the desired view from the dropdown menu. Standard and SNMP browsers can be selected.
Online Help	**Online Help**: Click this button if you want help with the menu now active. The description of the sub-menu where you are now is displayed.
Logout	**Logout**: If you want to end the configuration, click this button to log out of your device. A window is opened offering you the following options: • Save configuration, backup previous boot configuration, then exit. • Save configuration, then exit. • Exit without saving.

Navigation bar

Fig. 27: Save Configuration button

Fig. 28: Menus

The **Save Configuration** button is found in the navigation bar.

If you save a current configuration, you can save this as the boot configuration or you can also archive the previous boot configuration as a backup.

If you click the **Save configuration** button in the FCI, you will be asked "Do you really want to save the current configuration as a boot configuration?"

You have the following two options:

- *Save configuration*, i.e. save the current configuration as the boot configuration
- *Save configuration and backup previous boot configuration*, i.e. save the current configuration as the boot configuration and also archive the previous boot configuration as a backup.

If you want to load the archived boot configuration into your device, go to **Maintenance** -> **Software & Configuration** and select **Action** = *Restore Backup*. The archived backup is used as the current boot configuration.

The navigation bar also contains the main configuration menus and their sub-menus.

Click the main menu you require. The corresponding sub-menu then opens.

If you click the sub-menu you want, the entry selected will be displayed in red. All the other sub-menus will be closed. You can see at a glance the sub-menu you are in.

Status page

If you call the **Funkwerk Configuration Interface**, after you log in the status page of your device is displayed. The most important data of your device can be seen on this at a glance.

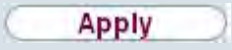
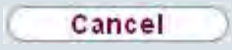
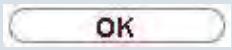
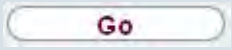
Main configuration window

The sub-menus generally contain several pages. These are called using the buttons at the top of the main window. If you click a button, the window is opened with the basic parameters. You can extend this by clicking the **Advanced Settings** tab, which displays the additional options.

Configuration elements

The various actions that you can perform when configuring your device in the **Funkwerk Configuration Interface** are triggered by means of the following buttons:

Funkwerk Configuration Interface buttons

Button	Function
	Updates the view.
	If you do not want to save a newly configured list entry, cancel this and any settings made by pressing **Cancel**.
	Confirms the settings of a new entry and the parameter changes in a list.
	Immediately starts the configured action.
	Calls the the sub-menu to create a new entry.
	Inserts an entry in an internal list.

Funkwerk Configuration Interface buttons for special functions

Button	Function
	In the **Access Point Search** menu, you use this button to start

Button	Function
	automatic detection of all the access points available and connected by Ethernet in the network.
Import	In the **System Management** -> **Certificates** -> **Certificates** and the **System Management** -> **Certificates** -> **CRLs** menus, this button opens the sub-menus for configuring the certificates or CRL imports.
Request	In the **System Management** -> **Certificates** -> **Certificates** menu, this button opens the sub-menu for the configuration of the certificate request.
Release Call	In the **Surveillance** -> **ISDN/Modem** -> **Current Calls** menu, clicking on this button ends the active calls selected in the column .

Various icons indicate the following possible actions or statuses:

Funkwerk Configuration Interface symbols

Icon	Function
	Deletes the list entry.
	Displays the menu for changing the settings of an entry.
	Displays the details for an entry.
	Moves an entry. A combo box opens in which you can choose the list entry that selected entry is to be be placed in front of/ after.
	Creates another list entry first and opens the configuration menu.
	Sets the status of the entry to `Inactive`.
	Sets the status of the entry to `Active`.
	Indicates "Dormant" status for an interface or connection.
	Indicates "Up" status for an interface or connection.
	Indicates "Down" status for an interface or connection.
	Indicates "Blocked" status for an interface or connection.
	Indicates "Going up" status for an interface or connection.
	Indicates that data traffic is encrypted.

Icon	Function
	Triggers a WLAN bandscan.
	Displays the next page in a list.
	Displays the previous page in a list.

You can select the following operating functions in the list view:

Funkwerk Configuration Interface list options

	Function
Update Interval	Here you can set the interval in which the view is to be updated. To do this, enter a period in seconds in the input field and confirm it with Apply.
Filter	You can have the list entries filtered and displayed according to certain criteria. You can determine the number of entries displayed per page by entering the required number in **View x per Page**. Use the « and » buttons to scroll one page forward and one page back. You can filter according to certain keywords within the configuration parameters by selecting the filter rule you want under **Filter in x <Option> y** and entering the search word in the input field. GO starts the filter operation.
Configuration elements	Some lists contain configuration elements. You can therefore change the configuration of the corresponding list entry directly in the list.

Fig. 29: Configuration of the update interval

Fig. 30: Filter list

Structure of the Funkwerk Configuration Interface configuration menu

The menus of the **Funkwerk Configuration Interface** contain the following basic structures:

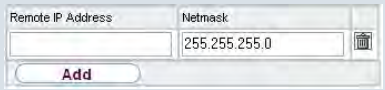
Funkwerk Configuration Interface Menu architecture

	Function
Basic configuration menu/list	When you select a menu from the navigation bar, the menu of basic parameters is displayed first. In a sub-menu containing several pages, the menu containing the basic parameters is displayed on the first page. The menu contains either a list of all the configured entries or the basic settings for the function concerned.
Sub-menu	The **New** button is available in each menu in which a list of all the configured entries is displayed. Click the button to display the configuration menu for creating a new list entry.
Sub-menu	Click this button to process the existing list entry. You go to the configuration menu.
Menu	Click this tab to display extended configuration options.

The following options are available for the configuration:

Funkwerk Configuration Interface configuration elements

	Function
Input fields	e.g. empty text field Text field with hidden input Enter the data.
Radio buttons	e.g. Select the corresponding option.
Checkboxes	e.g. activation by selecting checkbox Selection of several possible options

	Function
Dropdown menus	e.g. Click the arrow to open the list. Select the required option using the mouse.
Internal lists	e.g.  Click Add. A new list entry is created. Enter the corresponding data. If list input fields remain empty, these are not saved when you confirm with **OK**. Delete the entries by clicking the icon.

Display of options that are not available

Options that are not available because they depend on the selection of other options are generally hidden. If the display of these options could be helpful for a configuration decision, they are instead greyed out and cannot be selected.

Important

Please look at the messages displayed in the sub-menus. These provide information on any incorrect configurations.

Warning symbols

Icon	Meaning
	This symbol appears in messages referring you to settings that were made with the Setup Tool.
	This symbol appears in messages referring you to the fact that values were entered or selected incorrectly.

Pay particular attention to the following message:

"Warning: Changes not supported by the Setup Tool!" If you change them with the **Funkwerk Configuration Interface** , this can cause inconsistencies or malfunctions. Therefore, it is recommended that the configuration is continued with the Setup Tool.

7.3.1.3 Funkwerk Configuration InterfaceMenus

The configuration options of your device are contained in the sub-menus, which are displayed in the navigation bar in the left-hand part of the window.

Note

Please note that not all devices have the full range of functions. Check the software of your device on the corresponding product page under *www.funkwerk-ec.com* .

The **Funkwerk Configuration Interface** contains the following menus:

Assistants

Menu	Function
First steps	In this menu you can make the basic settings that are required to add your gateway to your local network (LAN).
Internet access	The wizard guides you through the individual configuration steps to connect your local network (LAN) to the internet.
VPN	In this menu you are guided through all of the settings that are required to set up your LAN-LAN connection as a virtual private network.
Wireless LAN	Wireless LAN involves the set-up of a network using wireless technology.
VoIP PBX in LAN	The assistant is required, e.g. for specific PBX in the LAN, such as **Hybird** in order to guarantee SIP compatibility. To do this, external communication is carried out over a single IP address and NAT is realised as full-cone NAT.

System Management

Menu	Function
Status	In this menu, general information on your device is displayed at a glance. This information includes serial number, software version, current memory and processor use, status of the physical interfaces and the last 10 system messages.
Global Settings	In this menu, you enter the basic system settings of your device, such as, for example, system name, system date, system time and passwords.

Menu	Function
	You can also manage licences that are necessary for the use of certain functions.
Interface Mode / Bridge Groups	In this menu, you define the mode in which the interfaces of your device are to run (routing or bridging) and if necessary can define bridge groups.
Administrative Access	In this menu, you configure the access options for the individual interfaces.
Remote Authentication	In this menu, you configure the authentication via a RADIUS server or TACAS+ server.
Certificates	In this menu you can generate and import keys and have them certified.

Physical Interfaces

Menu	Function
Ethernet Ports	In this menu, you configure the Ethernet interfaces of your device. To do this, you select the speed and type of interface, for example.
Serial Port	This menu is for configuring the serial interface if one exists.
Relay	In this menu, you configure the relay.

LAN

Menu	Function
IP configuration	In this menu, you carry out the IP configuration of the LAN interfaces for your device.
VLAN	In this menu, you configure the VLANs.

Wireless LAN

Menu	Function
WLAN	In this menu, you configure your wireless modules as an access point or bridge.
Administration	In this menu, you make the basic WLAN settings.

Wireless LAN Controller

Menu	Function
Wizard	The Wizard helps you to set up a WLAN infrastructure.
Controller Configuration	In this menu, you make the basic wireless LAN controller settings.
Slave AP Configuration	In this menu, you configure the slave access points.
Monitoring	In this menu, you can monitor active and neighbouring clients.
Maintenance	In this menu, you can update access point software and save any configurations.

Routing

Menu	Function
Routes	In this menu, you enter additional routes.
NAT	In this menu, you configure the NAT firewall (NAT, Network Address Translation).
RIP	In this menu, you configure the dynamic updating of the routing table via RIP.
Load Balancing	In this menu, you configure application-controlled bandwidth management.
Multicast	In this menu, you configure the use of multimedia streaming protocols for e.g. voice over IP or video and audio streaming (e.g. IPTV or Webradio) or TriplePlay (voice, video, data).
QoS	In this menu, you configure all the "Quality of Service" settings.

WAN

Menu	Function
Internet + Dialup	In this menu, you define the Internet connections for the various connection protocols or dialup connections.
Real Time Jitter Control	In this menu, you can set the upstream speed.

VPN

Menu	Function
IPSec	In this menu, you configure VPN connections over IPSec.
L2TP	In this menu you configure the use of L2TP (Layer 2 Tunnelling Protocol).
GRE	This menu shows a list of all configured GRE tunnels.

Firewall

Menu	Function
Policies	In this menu you configure the filter rules for the firewall.
Interfaces	In this menu, you can group together the interfaces to be filtered.
Addresses	In this menu, you can create the address aliases to be filtered.
Services	In this menu, you can create the service aliases to be filtered.

Local Services

Menu	Function
DNS	In this menu, you configure the name resolution.
HTTPS	In this menu, you configure the port and certificate for a configuration session over HTTPS.
DynDNS Client	In this menu, you configure the dynamic name resolution.
DHCP Server	In this menu, you configure your device as a DHCP server.
Scheduling	In this menu, you configure time-dependent standard actions of your devices.
Surveillance	In this menu, you configure the surveillance of interfaces or hosts in the network.
Funkwerk Discovery	In this menu, you can configure management functions for **bintec** Access Point.
Hotspot Gateway	In this menu, you configure the bintec Hotspot Gateway.

Maintenance

Menu	Function
Diagnostics	In this menu you can test the accessibility of hosts, DNS servers or routing.
Software & Configuration	In this menu, you can manage your device's configuration files. You can save them either locally on your device or on your computer, for example. you can start an update of the system software, the ADSL logic and the BOOTmonitor.
Reboot	In this menu, you can initiate the rebooting of the device.

External Reporting

Menu	Function
Syslog	In this menu, you configure the host to which the data logged internally on the device is forwarded for saving and further processing.
IP Accounting	In this menu, you decide for which interfaces accounting messages are to be generated.
E-mail Alert	Depending on the configuration, in this menu e-mails are sent to the administrator as soon as relevant syslog messages occur.
SNMP	In this menu, you configure whether the device is to listen for external SNMP accesses and send SNMP traps.
Activity Monitor	In this menu, you configure the surveillance of your device with the Windows Tool Activity Monitor (component of **BRICKware** for Windows).

Monitoring

Menu	Function
Internal Log	In this menu, the system messages are displayed.
IPSec	In this menu, the IPSec connections and connection statistics that are currently active are displayed.
Interfaces	In this menu, connection statistics and status of all interfaces are displayed.

Menu	Function
WLAN	This menu shows you the WLAN connections statistics.
Bridges	In this menu you can view the current values of the configured bridges.
Hotspot Gateway	This menu shows a list of all bintec Hotspot users.
QoS	In this menu, statistics are displayed for all interfaces for which QoS has been configured.

7.3.2 SNMP shell

SNMP (Simple Network Management Protocol) is a protocol that defines how you can access the configuration settings.

All configuration settings are stored in the MIB (Management Information Base) in the form of MIB tables and MIB variables. You can access these directly from the SNMP shell via SNMP commands. This type of configuration requires a detailed knowledge of our devices.

7.4 BOOTmonitor

The BOOTmonitor is only available over a serial connection to the device.

The BOOTmonitor provides the following functions, which you select by entering the corresponding number:

(1) Boot System (reboot the system):
The device loads the compressed boot file from the flash memory to the working memory. This happens automatically on starting.

(2) Software Update via TFTP:
The devices performs a software update via a TFTP server.

(3) Software Update via XMODEM:
The device performs a software update via a serial interface with XMODEM.

(4) Delete configuration:
The device is reset to the ex works state. All configuration files are deleted and the BOOTmonitor settings are set to the default values.

(5) Default BOOTmonitor Parameters:
You can change the default settings of the BOOTmonitor of the device, e.g. the baud rate for serial connections.

(6) Show System Information:
Shows useful information about your device, e.g. serial number, MAC address and software versions.

The BOOTmonitor is started as follows.

The devices passes through various functional states when starting:

- Start Mode
- BOOTmonitor mode
- Normal mode

After some self-tests have been successfully carried out in the start mode, your device reaches the BOOTmonitor mode. The BOOTmonitor prompt is displayed if you are serially connected to your device.

```
Press <sp> for boot monitor or any other key to boot system


W1002 Bootmonitor V.7.9.1 Rev. 1 from 2009/10/19 00:00:00
Copyright (c) 1996-2005 by Funkwerk Enterprise Communications GmbH

(1) Boot System
(2) Software Update via TFTP
(3) Software Update via XMODEM
(4) Delete Configuration
(5) Default Bootmonitor Parameters
(6) Show System Information

Your Choice> _
```

Fig. 31: BOOTmonitor

After display of the BOOTmonitor prompt, press the space bar within four seconds to use the functions of the BOOTmonitor. If you do not make an entry within four seconds, the device changes back to normal operating mode.

Note

If you change the baud rate (the preset value is 9600 baud), make sure the terminal program used also uses this baud rate. If this is not the case, you will not be able to establish a serial connection to the device.

Chapter 8 Assistants

The **Assistants** menu offers step-by-step instructions for the following basic configuration tasks:

- First steps
- Internet access
- VPN
- Wireless LAN
- VoIP PBX in LAN

Choose the corresponding task from the navigation bar and follow the instructions and explanations on the separate pages of the Assistant.

Chapter 9 System Management

The System Management menu contains general system information and settings.

You see a system status overview. Global system parameters such as the system name, date/time, passwords and licences are managed and the access and authentication methods are configured.

9.1 Status

If you log into the **Funkwerk Configuration Interface**, your device's status page is displayed, which shows the most important system information.

You see an overview of the following data:

- System status
- Your device's activities: Resource utilisation, active sessions and tunnels
- Status and basic configuration of LAN, WAN and WLAN interfaces
- The last 10 system messages

You can customise the update interval of the status page by entering the desired period in seconds as **Automatic Update Interval** and clicking on the **Apply**-button.

Caution

Under **Automatic Refresh Interval** do not enter a value of less than *5* seconds, otherwise the refresh interval of the screen will be too short to make further changes!

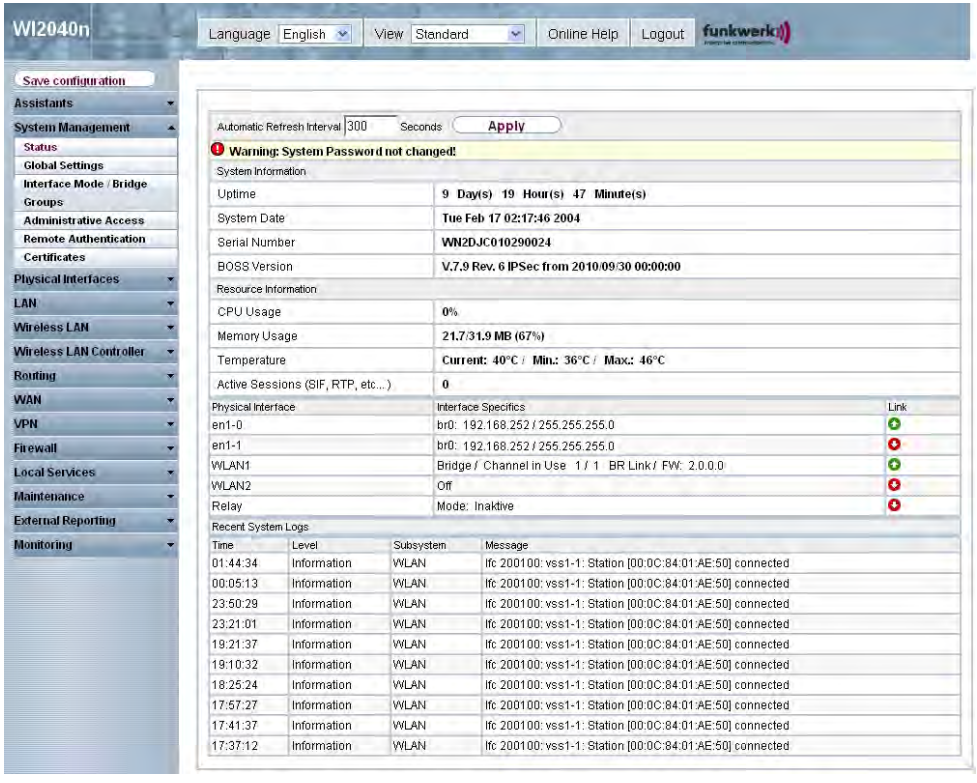

WI2040n
Language English
View Standard
Online Help
Logout
funkwerk
Save configuration
Assistants
System Management
Status
Global Settings
Interface Mode / Bridge Groups
Administrative Access
Remote Authentication
Certificates
Physical Interfaces
LAN
Wireless LAN
Wireless LAN Controller
Routing
WAN
VPN
Firewall
Local Services
Maintenance
External Reporting
Monitoring
Automatic Refresh Interval 300 Seconds Apply
Warning: System Password not changed!
System Information
Uptime 9 Day(s) 19 Hour(s) 47 Minute(s)
System Date Tue Feb 17 02:17:46 2004
Serial Number WN2DJC010290024
BOSS Version V.7.9 Rev. 6 IPSec from 2010/09/30 00:00:00
Resource Information
CPU Usage 0%
Memory Usage 21.7/31.9 MB (67%)
Temperature Current: 40°C / Min.: 36°C / Max.: 46°C
Active Sessions (SIP, RTP, etc...) 0
Physical Interface Interface Specifics Link
en1-0 br0: 192.168.252 / 255.255.255.0
en1-1 br0: 192.168.252 / 255.255.255.0
WLAN1 Bridge / Channel in Use 1 / 1 BR Link / FW: 2.0.0.0
WLAN2 Off
Relay Mode: Inaktive
Recent System Logs
Time Level Subsystem Message
01:44:34 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
00:05:13 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
23:50:29 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
23:21:01 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
19:21:37 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
19:10:32 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
18:25:24 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
17:57:27 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
17:41:37 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected
17:37:12 Information WLAN Ifc 200100: vss1-1: Station [00:0C:84:01:AE:50] connected

Fig. 32: **System Management** -> **Status**

The **System Management** -> **Status** menu consists of the following fields:

Fields in the Status System Information menu

Field	Value
Uptime	Displays the time past since the device was rebooted.
System Date	Displays the current system date and system time.
Serial Number	Displays the device serial number.
BOSS Version	Displays the currently loaded version of the system software.

Fields in the Status Resource Information menu

Field	Value
CPU Usage	Displays the CPU usage as a percentage.
Memory Usage	Displays the usage of the working memory in MByte in relation to the available total working memory in MByte. The usage is also displayed in brackets as a percentage.
Temperature	Devices of the **bintec WI** series are fitted with a temperature

Field	Value
	sensor. This shows the current temperature and the maximum and minimum temperatures reached.
Active Sessions (SIF, RTP, etc...)	Displays the total of all SIF, TDRC, and IP load balancing sessions.
Active IPSec Tunnels	Displays the number of currently active IPSec tunnels in relation to the number of configured IPSec tunnels.

Other fields in the menu Status

Field	Value
Physical Interface - Interface Specifics - Link	The physical interfaces are listed here and their most important settings are shown. The system also displays whether the interface is connected or active. Interface specifics for Ethernet interfaces: • IP address • Netmask Interface specifics for serial/ISDN interfaces: • Configured • Not configured Interface specifics for xDSL interfaces: • Downstream/Upstream Line Speed Interface Specifics for WLAN Interfaces: Access Point Mode: • Operation Mode: Access Point or Off • The channel used on this wireless module • Number of connected clients • Number of WDS links • Software version of the wireless card Access Client Mode: • Operation Mode: Access Client or Off • The channel used on this wireless module

Field	Value
	• Software version of the wireless card Bridge mode: • Operation Mode: Bridge or Off • The channel used on this wireless module • Number of configured bridge links • Software version of the wireless card Interface specifics for relay: • Configured Mode
Recent System Logs	Displays the last 10 system messages.

9.2 Global Settings

The basic system parameters are managed in the **Global Settings** menu.

9.2.1 System

The **System Management** -> **Global Settings** -> **System** menu is used for entering the basic system data of your device.

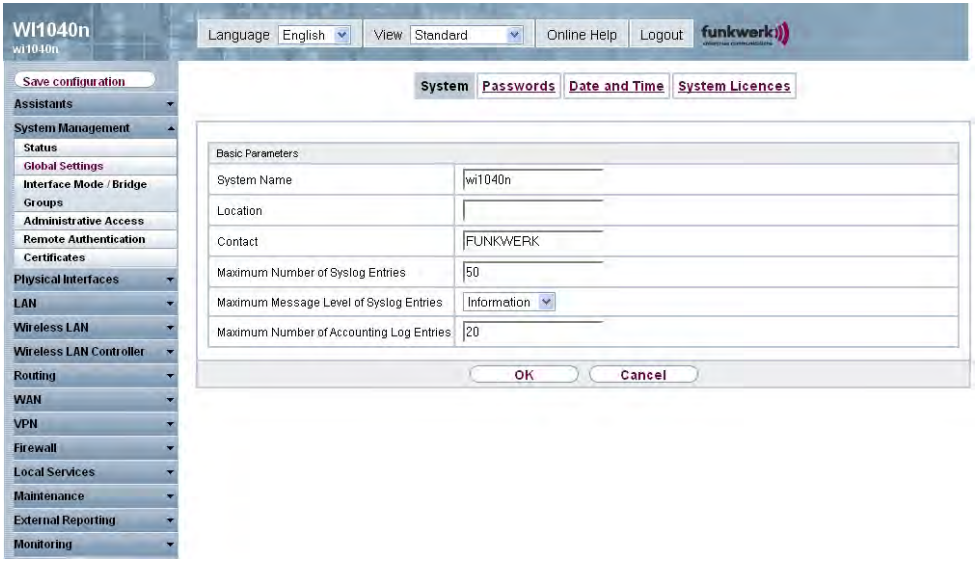


Fig. 33: **System Management** -> **Global Settings** -> **System**

The **System Management** -> **Global Settings** -> **System** menu consists of the following fields:

Fields in the System Basic Parameters menu

Field	Value
System Name	Enter the system name of your device. This is also used as the PPP host name. A character string of up to 255 characters is possible. The device type is entered as the default value.
Location	Enter the location of your device.
Contact	Enter the relevant contact person. Here you can enter the e-mail address of the system administrator, for example. A character string of up to 255 characters is possible. The default value is *FUNKWERK*.
Maximum Number of Syslog Entries	Enter the maximum number of syslog messages that are stored internally in the device. Possible values are *0* to *1000*.

Field	Value
	The default value is *50*. You can view the stored messages in **Monitoring** -> **Internal Log**.
Maximum Message Level of Syslog Entries	Select the priority of system messages above which a log should be created. System messages are only recorded internally if they have a higher or identical priority to that indicated, i.e. all messages generated are recorded at syslog level *debug*. Possible values: • *Emergency*: Only messages with emergency priority are recorded. • *Alert*: Messages with emergency and alert priority are recorded. • *Critical*: Messages with emergency, alert and critical priority are recorded. • *Errors*: Messages with emergency, alert, critical and error priority are recorded. • *Warning*: Messages with emergency, alert, critical, error and warning priority are recorded. • *Notice*: Messages with emergency, alert, critical, error, warning and notice priority are recorded. • *Information* (default value) Messages with emergency, alert, critical, error, warning, notice and information priority are recorded. • *Debug*: All messages are recorded.
Maximum Number of Accounting Log Entries	Enter the maximum number of accounting entries that are stored internally in the device. Possible values are *0* to *1000*. The default value is *20*.

9.2.2 Passwords

Setting the passwords is another basic system setting.

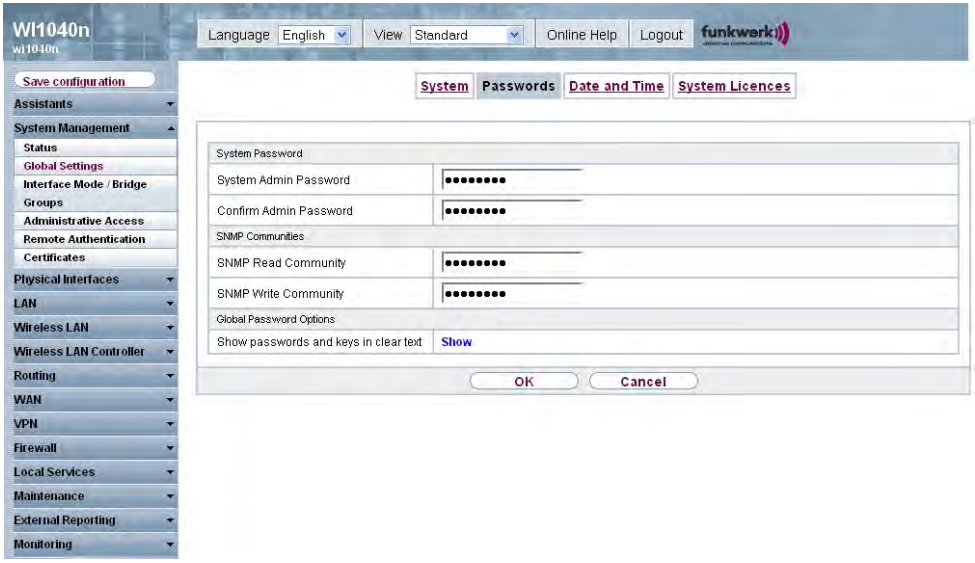


Fig. 34: **System Management** -> **Global Settings** -> **Passwords**

Note

All **bintec** devices are delivered with the same username and password. As long as the password remains unchanged, they are not protected against unauthorised use.

Make sure you change the passwords to prevent unauthorised access to the device

If the password is not changed, under **System Administration** -> **Status** appears the warning: "System password not changed!"

The **System Management** -> **Global Settings** -> **Passwords** menu consists of the following fields:

Fields in the Passwords System Password menu

Field	Value
System Admin Password	Enter the password for the user name `admin`. This password is also used with SNMPv3 for authentication (MD5) and encryption (DES).
Confirm Admin Password	Confirm the password by entering it again.

Fields in the Passwords SNMP Communities menu

Field	Value
SNMP Read Community	Enter the password for the user name `read`.
SNMP Write Community	Enter the password for the user name `write`.

Fields in the Passwords Global Password Options menu

Field	Value
Show passwords and keys in clear text	Define whether the passwords are to be displayed in clear text (plain text). The function is activated with *Show*. The function is disabled by default. If you activate the function, all passwords and keys in all menus are displayed and can be edited in plain text. The WLAN and IPSec keys are one exception here. They can only be entered in plain text. If you press **OK** or call the menu again, they are displayed as asterisks.

9.2.3 Date and Time

You need the system time for tasks such as correct timestamps for system messages, accounting or IPSec certificates.

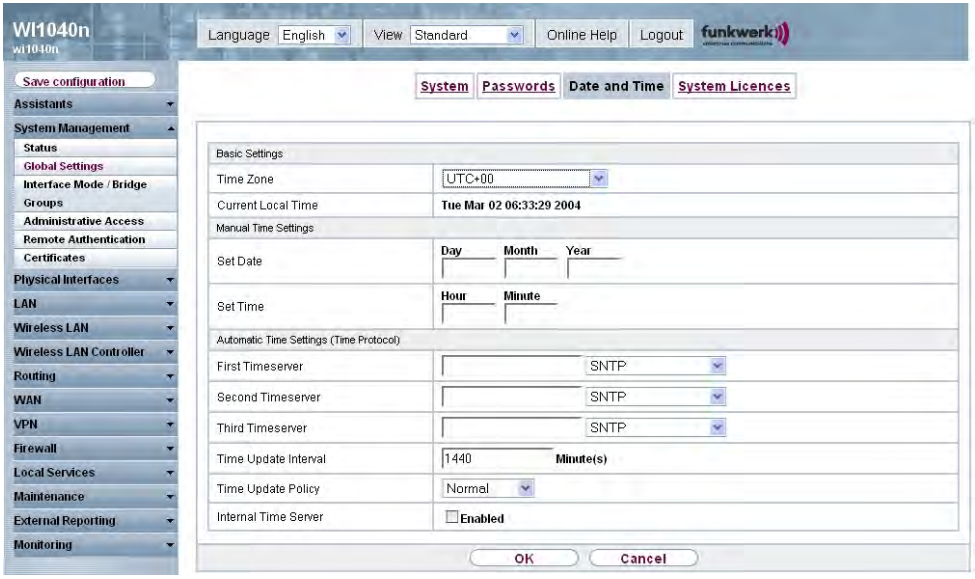


Fig. 35: **System Management** -> **Global Settings** -> **Date and Time**

You have the following options for determining the system time (local time):

Manual

The system time can be set manually on the device.

If the correct location of the device (country/city) is set for the **System Time Zone**, switching from summer time to winter time (and back) is automatic. The switch occurs independently of an NTP server. Summer time starts on the last Sunday in March by switching from 2 a.m. to 3 a.m. The calendar-related or schedule-related switches that are scheduled for the missing hour are then carried out. Winter time starts on the last Sunday in October by switching from 3 a.m. to 2 a.m. The calendar-related or schedule-related switches that are scheduled for the additional hour are then carried out.

If a value other than Universal Time Coordinated (UTC), option `UTC+-x`, has been chosen for the **System Time Zone**, the switch from summer to winter time must be carried out manually when required.

Time server

You can obtain the system time automatically, e.g. using various time servers. To ensure that the device uses the desired current time, you should configure one or more time servers. Switching from summer time to winter time (and back) must be carried out manually if the time is derived using this method by changing the value in the **System Time Zone** field with an option UTC+ or UTC-.

Note

If a method for automatically deriving the time is defined on the device, the values obtained in this way automatically have higher priority. A manually entered system time is therefore overwritten.

The **System Management** -> **Global Settings** -> **Date and Time** menu consists of the following fields:

Fields in the Date and Time Basic Settings menu

Field	Description
Time Zone	Select the time zone in which your device is installed. You can select Universal Time Coordinated (UTC) plus or minus the deviation in hours or a predefined location, e.g. *Europe/Berlin*.
Current Local Time	The current date and current system time are shown here. The entry cannot be changed.

Fields in the Date and Time Manual Time Settings menu

Field	Description
Set Date	Enter a new date. Format: • **Day**: dd • **Month**: mm • **Year**: yyyy
Set Time	Enter a new time. Format: • **Hour**: hh • **Minute**: mm

Fields in the Date and Time Automatic Time Settings (Time Protocol) menu

Field	Description
First Timeserver	Enter the primary time server, using either a domain name or an

Field	Description
	IP address. In addition, select the protocol for the time server request. Possible values: • *SNTP* (default value): This server uses the simple network time protocol with UDP port 123. • *Time Service / UDP*: This server uses the Time service with UDP port 37. • *Time Service / TCP*: This server uses the Time service with TCP port 37. • *None*: This time server is not currently used for the time request.
Second Timeserver	Enter the secondary time server, using either a domain name or an IP address. In addition, select the protocol for the time server request. Possible values: • *SNTP* (default value): This server uses the simple network time protocol with UDP port 123. • *Time Service / UDP*: This server uses the Time service with UDP port 37. • *Time Service / TCP*: This server uses the Time service with TCP port 37. • *None*: This time server is not currently used for the time request.
Third Timeserver	Enter the tertiary time server, using either a domain name or an IP address. In addition, select the protocol for the time server request. Possible values: • *SNTP* (default value): This server uses the simple network time protocol with UDP port 123. • *Time Service / UDP*: This server uses the Time service with UDP port 37.

Field	Description
	• *Time Service / TCP*: This server uses the Time service with TCP port 37. • *None*: This time server is not currently used for the time request.
Time Update Interval	Enter the time interval in minutes at which the time is automatically updated. The default value is *1440*.
Time Update Policy	Enter the time period after which the system attempts to contact the time server again following a failed time update. Possible values: • *Normal* (default value): The system attempts to contact the time server after 1, 2, 4, 8, and 16 minutes. • *Aggressive*: For ten minutes, the system attempts to contact the time server after 1, 2, 4, 8 seconds and then every 10 seconds. • *Endless*: For an unlimited period, the system attempts to contact the time server after 1, 2, 4, 8 seconds and then every 10 seconds. If certificates are used to encrypt data traffic in a VPN, it is extremely important that the correct time is set on the device. To ensure this is the case, for **Time Update Policy**, select the value *Endless*.
Internal Timeserver	Select whether the internal timeserver is to be used. The function is activated by choosing *Enabled*. Time requests from a client will be answered with the current system time. This is given as GMT, without offset. The function is disabled by default. Time requests from a client are not answered.

9.2.4 System Licences

This chapter describes how to activate the functions of the software licences you have purchased.

The following licence types exist:

- Licences already available in the device's ex works state
- Free extra licences
- Extra licences at additional cost

The data sheet for your device tells you which licences are available in the device's ex works state and which can also be obtained free of charge or at additional cost. You can access this data sheet at *www.funkwerk-ec.com*.

You can obtain the licence data for extra licences via the online licensing pages in the support section at *www.funkwerk-ec.com*. Please follow the online licensing instructions. (Please also note the information on the licence card for licences at additional cost.) You will then receive an e-mail containing the following data:

- **License Key** and
- **Licence Serial Number**

You enter this data in the **System Management** -> **Global Settings**-> **System Licenses** -> **New** menu.

In the **System Management** -> **Global Settings** ->**System Licenses** menu, a list of all registered licenses is shown (**Description**, **License Type**, **License Serial Number**, **Status**).

Possible values for Status:

Licence	Meaning
OK	Subsystem is activated.
Not OK	Subsystem is not activated.
Not supported	You have entered a licence for a subsystem your device does not support.

In addition, above the list is shown the **System License-ID** required for on-line licensing.

Note

To restore the standard licences for a device, click the **Default Licences** (standard licences) button.

9.2.4.1 Edit/New

Choose the icon to edit existing entries. Choose the **New** button to add licences.

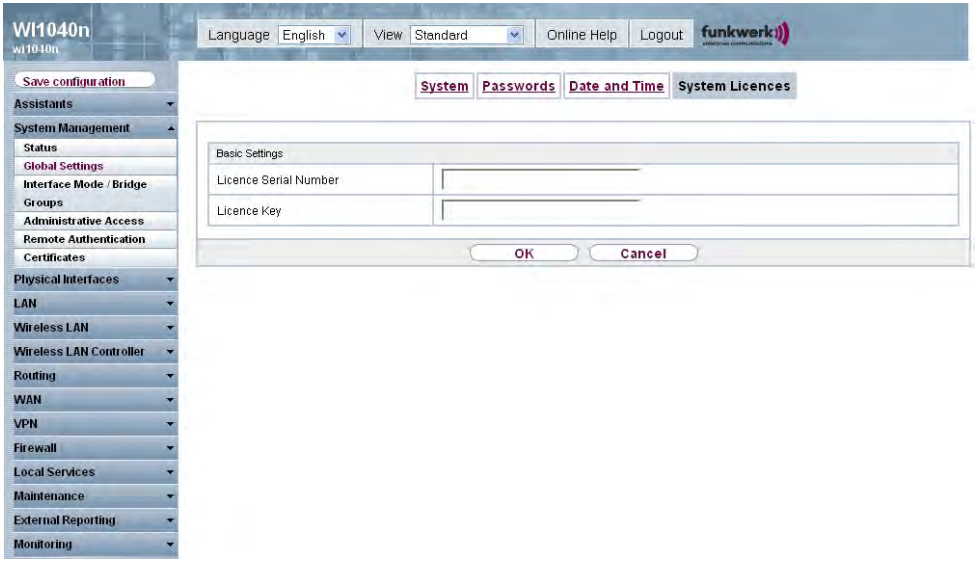


Fig. 36: **System Management** -> **Global Settings** -> **System Licenses** -> **New**

Activating extra licences

You activate extra licences by adding the received licence information in the **System Management** -> **Global Settings** -> **System Licenses** -> **New** menu.

The **System Management** -> **Global Settings** -> **System Licences** -> **New** menu consists of the following fields:

Fields in the System Licences Basic Settings menu

Field	Value
Licence Serial Number	Enter the licence serial number you received when you bought the licence.
Licence Key	Enter the licence key you received by e-mail.

Note

If `Not OK` is displayed as the status:

- Enter the licence data again.
- Check your hardware serial number.

If `Not Supported` is displayed as the status, you have entered a license for a subsystem that your device does not support. This means you cannot use the functions of this licence.

Deactivating a licence

Proceed as follows to deactivate a licence:

(1) Go to **System Management** -> **Global Settings** -> **System Licenses**.

(2) Press the icon in the line containing the licence you want to delete.

(3) Confirm with **OK**.

The licence is deactivated. You can reactivate your additional licence at any time by entering the valid licence key and licence serial number.

9.3 Interface Mode / Bridge Groups

In this menu, you define the operation mode for your device's interfaces.

Routing versus bridging

Bridging connects networks of the same type. In contrast to routing, bridges operate at layer 2 of the OSI model (data link layer), are independent of higher-level protocols and transmit data packets using MAC addresses. Data transmission is transparent, which means the information contained in the data packets is not interpreted.

With routing, different networks are connected at layer 3 (network layer) of the OSI model and information is routed from one network to the other.

Conventions for port/interface names

If your device has a radio port, it receives the interface name WLAN. If there are several radio modules, the names of wireless ports in the user interface of your device are made up of the following parts:

(a) WLAN

(b) Number of the physical port (1 or 2)

Example: *WLAN1*

The name of the Ethernet port is made up of the following parts:

(a) ETH, where en stands for Ethernet

(b) Number of the port

Example: *ETH1*

The names of the interfaces connected to an Ethernet port are made up of the following parts:

(a) Abbreviation for interface type

(b) Number of the Ethernet port

(c) Number of the interface

Example: *en1-0* (first interface on the first Ethernet port)

The name of the bridge group is made up of the following parts:

(a) Abbreviation for interface type

(b) Number of the bridge group

Example: *br0* (first bridge group)

The name of the wireless network is made up of the following parts:

(a) Abbreviation for interface type

(b) Number of the wireless module

(c) Number of the interface

Example: *vss1-0* (first wireless network on the first wireless module)

The name of the WDS link or bridge link is made up of the following parts:

(a) Abbreviation for interface type

(b) Number of the wireless module on which the WDS link or bridge link is configured

(c) Number of the WDS link or bridge link

Example: *wds1-0* (first WDS link or bridge link on the first wireless module)

The name of the client link is made up of the following parts:

(a) Abbreviation for interface type

(b) Number of the wireless module on which the client link is configured

(c) Number of the client link

Example: *sta1-0* (first client link on the first wireless module)

The names of the virtual interfaces connected to an Ethernet port are made up of the following parts:

(a) Abbreviation for interface type

(b) Number of the Ethernet port

(c) Number of the interface connected to the Ethernet port

(d) Number of the virtual interface

Example: `en1-0-1` (first virtual interface based on the first interface on the first Ethernet port)

9.3.1 Interfaces

You define separately whether each interface is to operate in routing or bridging mode.

If you want to set bridging mode, you can either use existing bridge groups or create a new bridge group.

The default setting for all existing interfaces is bridging mode. On selecting the `New Bridge Group` option for **Mode / Bridge Group**, a bridge group, i.e. `br1`, `br2` etc., is automatically created and the interface is run in bridging mode.

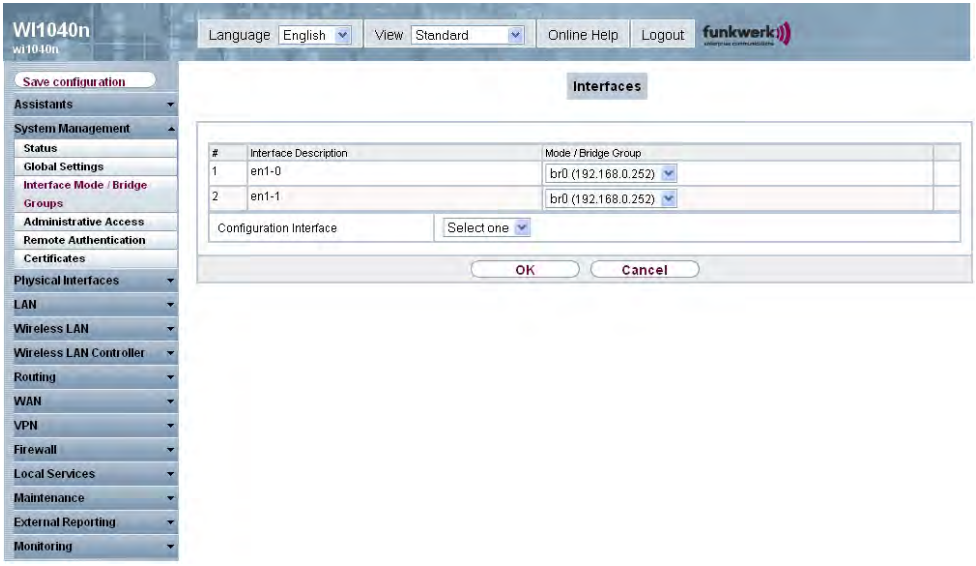


Fig. 37: **System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces**

The **System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces** menu consists of the following fields:

Fields in the Interfaces menu

Field	Description
#	Shows the serial number of the interface.

Field	Description
Interface Description	Displays the name of the interface.
Mode / Bridge Group	Select whether you want to run the interface in *Routing Mode* or whether you want to assign the interface to an existing (*br0*, *br1* etc.) or new bridge group (*New Bridge Group*). If you select *New Bridge Group*, a new bridge group is created automatically when you click **OK**.
Configuration Interface	Select the interface via which the configuration is to be carried out. Possible values: • *Select one* (default value): Ex works setting The right configuration interface must be selected from the other options. • *Ignore* : No interface is defined as configuration interface. • *<Interface name>*: Select the interface to be used for configuration. If this interface is in a bridge group, it is assigned the group's IP address when it is taken out of the group.

9.3.1.1 <stax-x> Edit

Click the icon to edit additional settings for WLAN clients in bridge mode (so-called MAC bridge).

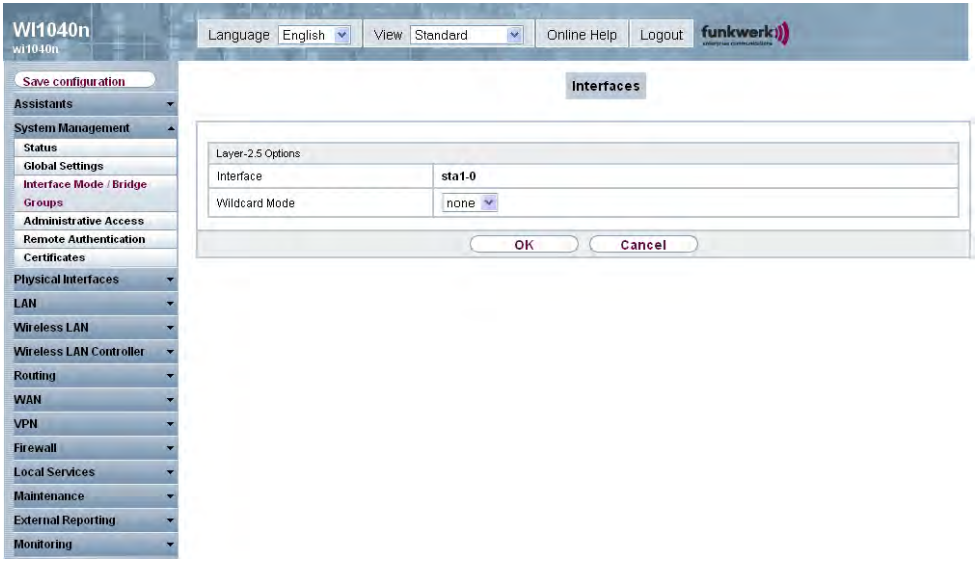


Fig. 38: **System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces** -> **Edit**

You can realise bridging for devices behind access clients with the MAC Bridge function. In wildcard mode you cannot define how Unicast non-IP frames or non-ARP frames are processed. To use the MAC bridge function, you must carry out configuration steps in several menus.

(1) Select the **Funkwerk Configuration Interface** menu **Wireless LAN** -> **WLAN** -> **Wireless Module Settings** and click the icon to change an entry.

(2) Set **Operation Mode** to *Access Client* and save the settings with **OK**.

(3) Select the menu options **System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces**. The additional interface **sta1-0** is displayed.

(4) For interface **sta1-0** select Mode / Bridge Group = *br0 (<IPAddress>)* and **Configuration Interface** = *en1-0* and save the settings with **OK**.

(5) Click the **Save Configuration** button to save all of the configuration settings. You can use the MAC Bridge.

The **System Management** -> **Interface Mode / Bridge Groups** -> **Edit** menu consists of the following fields:

Fields in the <stax-x> Layer 2.5 Option menu

Field	Value
Interface	Shows the interface that is being edited.
Wildcard Mode	Select the Wildcard mode you want to use on the interface. Possible values:

Field	Value
	• *None* (default value): Wildcard mode is not used. • *Static*: With this setting, you must enter the MAC address of a device that is connected over IP under **Wildcard MAC Address**. Each packet without IP and without ARP is forwarded to this device. This occurs even when the device is no longer connected. • *First*: If you choose this setting the MAC address of the first non-IP unicast frame or non-ARP unicast frame, which occurs on any of the Ethernet interfaces, is used as the wildcard MAC address. This wildcard MAC address can only be reset by rebooting the device or by selecting another wildcard mode. • *Last*: If you choose this setting the internal WLAN MAC address is used to establish a connection to the access point. As soon as a non-IP unicast frame or non-ARP unicast frame appears, it is forwarded to the MAC address from which the last non-IP unicast frame or non-ARP unicast frame was received on the Ethernet interface of the device. This wildcard MAC address is renewed with each non-IP unicast frame or non-ARP unicast frame.
Wildcard MAC Address	Only for **Wildcard Mode** = *Static* Enter the MAC address of a device that is connected over IP.
Transparent MAC Address	Only for **Wildcard Mode** = *Static*, *First* Choose whether or not the **Wildcard MAC Address** is used in addition to the WLAN MAC address to establish the connection to the access point. The function is activated with *Enabled*. The function is disabled by default.

9.4 Administrative Access

In this menu, you can configure the administrative access to the device.

9.4.1 Access

In the **Administrative Access** -> **Access** menu, a list of all IP-configurable interfaces is shown.

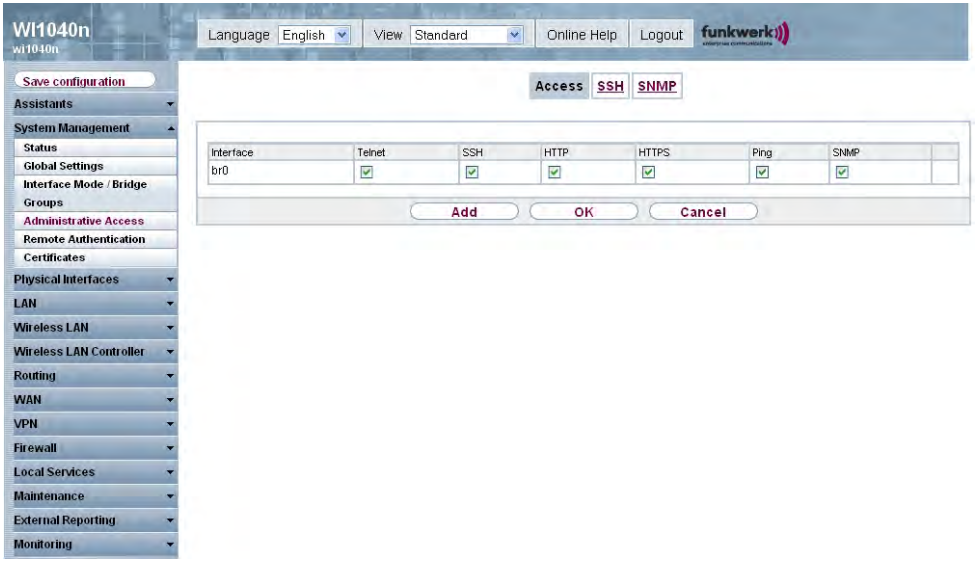


Fig. 39: **System Management** -> **Administrative Access** -> **Access**

For the Ethernet interface you can select the access parameters *Telnet*, *SSH*, *HTTP*, *HTTPS*

, *Ping* and *SNMP*.

9.4.1.1 Add

Press the **Add** button to configure administrative access for additional interfaces.

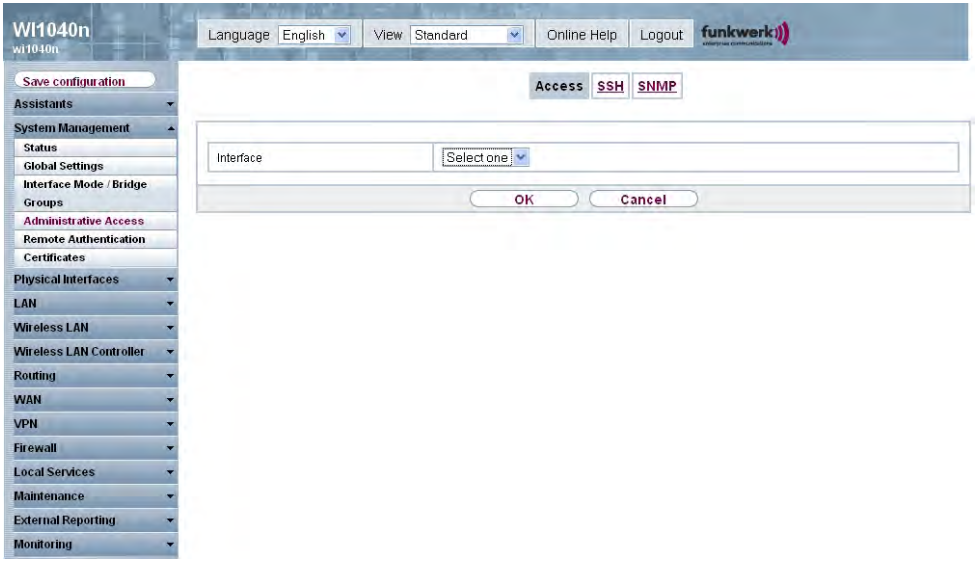


Fig. 40: **System Management** -> **Administrative Access** -> **Access** -> **Add**

The **System Management** -> **Administrative Access** -> **Access** -> **Add** menu consists of the following fields:

Fields in the Access menu

Field	Description
Interface	Select the interface for which administrative access is to be configured.

9.4.2 SSH

Your devices offers encrypted access to the shell. You can enable (**enabled**, default value) or disable this access in the **System Management** -> **Administrative Access** -> **SSH** menu and have access to the options for configuration of the SSH login.

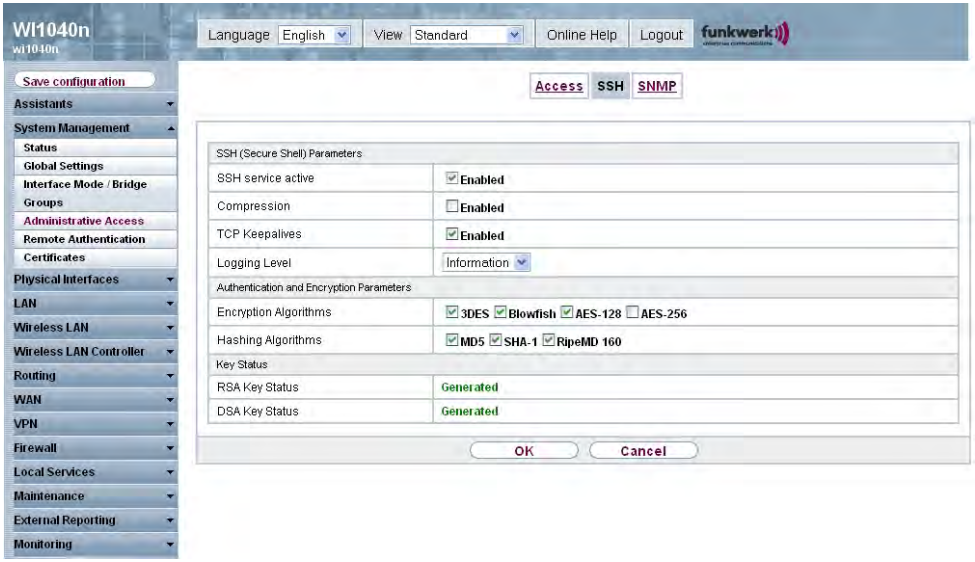


Fig. 41: **System Management** -> **Administrative Access** -> **SSH**

You need an SSH client application, e.g. PuTTY, to be able to reach the SSH Daemon.

If you wish to use SSH Login together with the PuTTY client, you may need to comply with some special configuration requirements, for which we have prepared FAQs. You will find these in the Service/Support section at *www.funkwerk-ec.com* .

To be able to reach the shell of your device via an SSH client, make sure the settings for the SSH Daemon and SSH client are the same.

Note

If configuration of an SSH connection is not possible, restart the device to initialise the SSH Daemon correctly.

The **System Management** -> **Administrative Access** -> **SSH** menu consists of the following fields:

Fields in the SSH SSH (Secure Shell) Parameters menu

Field	Value
SSH service active	Select whether the SSH Daemon is to be enabled for the interface. The function is activated by choosing `Enabled`.

Field	Value
	The function is enabled by default.
Compression	Select whether data compression should be used. The function is activated by choosing *Enabled*. The function is disabled by default.
TCP Keepalives	Select whether the device is to send keepalive packets. The function is activated by choosing *Enabled*. The function is enabled by default.
Logging Level	Select the syslog level for the syslog messages generated by the SSH Daemon. Possible settings: • *Information* (default value) Fatal and simple errors of the SSH Daemon and information messages are recorded. • *Fatal*: Only fatal errors of the SSH Daemon are recorded. • *Errors*: Fatal and simple errors of the SSH Daemon are recorded. • *Debug*: All messages are recorded.

Fields in the SSH Authentication and Encryption Parameters menu

Field	Value
Encryption Algorithms	Select the algorithms that are to be used to encrypt the SSH connection. Possible options: • *3DES* • *Blowfish* • *AES-128* • *AES-256* *3DES*, *Blowfish* and *AES-128* and are enabled by default.
Hashing Algorithms	Select the algorithms that are to be available for message authentication of the SSH connection.

Field	Value
	Possible options: • *MD5* • *SHA-1* • *RipeMD160* *MD5*, *SHA-1* and *RipeMD160* are enabled by default.

Fields in the SSH Key Status menu

Field	Value
RSA Key Status	Shows the status of the RSA key. If an RSA key has not been generated yet, *Not Generated* is displayed in red and a link, *Generate*, is provided. If you select the link, the generation process is triggered and the view is updated. The status *Generating* is displayed in green. When generation has been completed successfully, the status changes from *Generating* to *Generated*. If an error occurs during generated, *Not Generated* and the *Generate* link are displayed again. You can then repeat generation. If the status *Unknown* is displayed, generation of a key is not possible, for example because there is not enough space in the FlashROM.
DSA Key Status	Shows the status of the DSA key. If a DSA key has not been generated yet, *Not Generated* is displayed in red and a link, *Generate*, is provided. If you select the link, the generation process is triggered and the view is updated. The status *Generating* is displayed in green. When generation has been completed successfully, the status changes from *Generating* to *Generated*. If an error occurs during generated, *Not Generated* and the *Generate* link are displayed again. You can then repeat generation. If the status *Unknown* is displayed, generation of a key is not possible, for example because there is not enough space in the FlashROM.

9.4.3 SNMP

SNMP (Simple Network Management Protocol) is a network protocol used to monitor and control network elements (e.g. routers, servers, switches, printers, computers etc.) from a central station. SNMP controls communication between the monitored devices and monitoring station. The protocol describes the structure of the data packets that can be transmitted, as well as the communication process.

The data objects queried via SNMP are structured in tables and variables and defined in the MIB (Management Information Base). This contains all the configuration and status variables of the device.

SNMP can be used to perform the following network management tasks:

- Surveillance of network components
- Remote controlling and configuration of network components
- Error detection and notification

You use this menu to configure the use of SNMP.

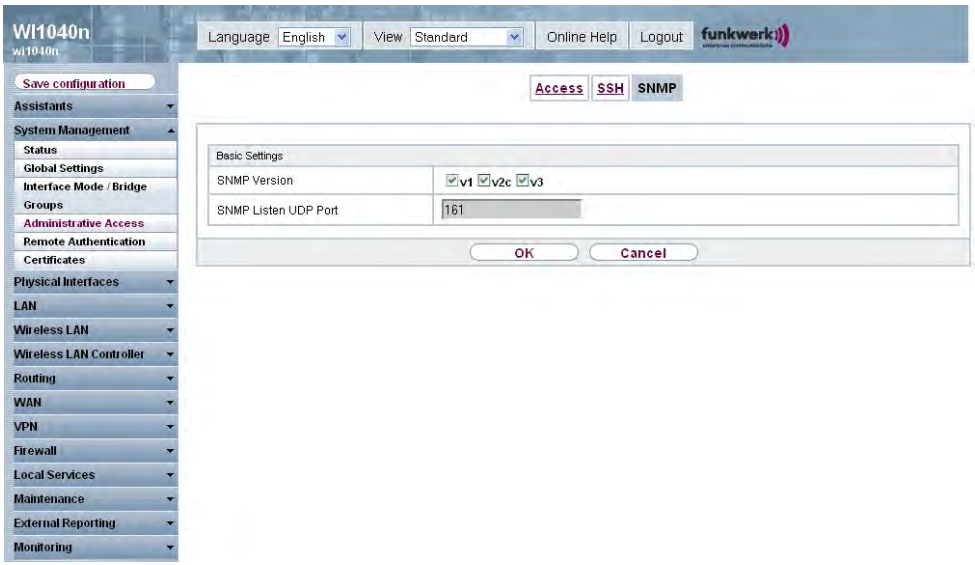


Fig. 42: **System Management** -> **Administrative Access** -> **SNMP**

The **System Management** -> **Administrative Access** -> **SNMP** menu consists of the following fields:

Fields in the SNMP Basic Settings menu

Field	Value
SNMP Version	Select the SNMP version your device is to use to listen for external SNMP accesses. Possible values: • *v1*: SNMP Version 1 • *v2c*: Community-Based SNMP Version 2 • *v3*: SNMP Version 3 *v1*, *v2c* and *v3* are active by default. If no option is selected, the function is deactivated.
SNMP Listen UDP Port	Shows the UDP port (*161*) at which the device receives SNMP requests. The value cannot be changed.

Tip

If your SNMP Manager supports SNMPv3, you should, if possible, use this version as older versions transfer all data unencrypted.

9.5 Remote Authentication

This menu contains the settings for user authentication.

9.5.1 RADIUS

RADIUS (Remote Authentication Dial In User Service) is a service that enables authentication and configuration information to be exchanged between your device and a RADIUS server. The RADIUS server administrates a database with information about user authentication and configuration and for statistical recording of connection data.

RADIUS can be used for:

- Authentication
- Accounting
- Exchange of configuration data

For an incoming connection, your device sends a request with user name and password to

the RADIUS server, which then searches its database. If the user is found and can be authenticated, the RADIUS server sends corresponding confirmation to your device. This confirmation also contains parameters (called RADIUS attributes), which your device uses as WAN connection parameters.

If the RADIUS server is used for accounting, your device sends an accounting message at the start of the connection and a message at the end of the connection. These start and end messages also contain statistical information about the connection (IP address, user name, throughput, costs).

RADIUS packets

The following types of packets are sent between the RADIUS server and your device (client):

Packet types

Field	Value
ACCESS_REQUEST	Client -> Server If an access request is received by your device, a request is sent to the RADIUS server if no corresponding connection partner has been found on your device.
ACCESS_ACCEPT	Server -> Client If the RADIUS server has authenticated the information contained in the ACCESS_REQUEST, it sends an ACCESS_ACCEPT to your device together with the parameters used for setting up the connection.
ACCESS_REJECT	Server -> Client If the information contained in the ACCESS_REQUEST does not correspond to the information in the user database of the RADIUS server, it sends an ACCESS_REJECT to reject the connection.
ACCOUNTING_START	Client -> Server If a RADIUS server is used for accounting, your device sends an accounting message to the RADIUS server at the start of each connection.
ACCOUNTING_STOP	Client -> Server

Field	Value
	If a RADIUS server is used for accounting, your device sends an accounting message to the RADIUS server at the end of each connection.

In the **System Management** -> **Remote Authentication** -> **RADIUS** menu, a list of all registered RADIUS servers is displayed.

9.5.1.1 Edit/New

Choose the icon to edit existing entries. Choose the **New** button to add RADIUS servers.

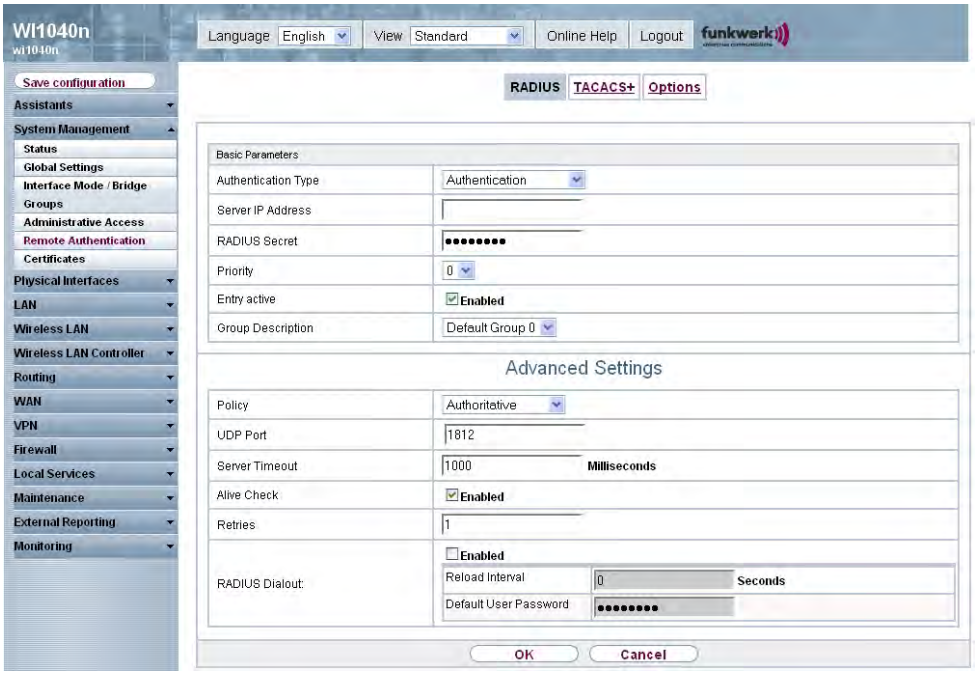


Fig. 43: **System Management** -> **Remote Authentication** -> **RADIUS** -> **New**

The **System Management** -> **Remote Authentication** -> **RADIUS** -> **New** menu consists of the following fields:

Fields in the RADIUS Basic Parameters menu

Field	Value
Authentication Type	Select what the RADIUS server is to be used for.

Field	Value
	Possible values: • *Authentication* (default value): The RADIUS server is used for controlling access to a network. • *Accounting*: The RADIUS server is used for recording statistical call data. • *Login Authentication*: The RADIUS server is used for controlling access to the SNMP shell of your device. • *IPSec Authentication*: The RADIUS server is used for sending configuration data for IPSec peers to your device. • *WLAN (802.1x)*: The RADIUS server is used for controlling access to a wireless network. • *XAUTH*: The RADIUS server is used for authenticating IPSec peers via XAuth.
Vendor Mode	Only for **Authentication Type** = *Accounting*. In hotspot applications, select the mode define by the provider. In standard application, leave the default value *Standard*. Possible values for hotspot applications: • *France Telecom*: For France Telecom hotspot applications. • *bintec HotSpot Server*: For bintec hotspot applications.
Server IP Address	Enter the IP address of the RADIUS server.
RADIUS Password	Enter the shared password used for communication between the RADIUS server and your device.
Priority	If a number of RADIUS server entries were created, the server with the highest priority is used first. If this server does not answer, the server with the next-highest priority is used. Possible values from *0* (highest priority) to *7* (lowest priority). The default value is *0*. See also **Policy** in the **Advanced Settings**.
Entry active	Select whether the RADIUS server configured in this entry is to be used.

Field	Value
	The function is activated by choosing *Enabled*. The function is enabled by default.
Group Description	Define a new RADIUS group description or assign the new RADIUS entry to a predefined group. The configured RADIUS servers for a group are queried according to **priority** and **policy**. Possible values: • *New*: Enter a new group description in the text field. • *Default Group 0*(default value): Select this entry for special applications, such as Hotspot Server configuration. • *<Group Name>*: Select a predefined group from the list.

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Value
Policy	Select how your device is to react if a negative response to a request is received. Possible values: • *Authoritative* (default value): A negative response to a request is accepted. • *Non-authoritative* : A negative response to a request is not accepted. A request is sent to the next RADIUS server until your device receives a response from a server configured as authoritative.
UDP Port	Enter the UDP port to be used for RADIUS data. RFC 2138 defines the default ports 1812 for authentication (1645 in older RFCs) and 1813 for accounting (4,180.84 cm older RFCs). You can obtain the port to be used from the documentation for your RADIUS server. The default value is *1812*.
Server Timeout	Enter the maximum wait time between ACCESS_REQUEST

Field	Value
	and response in milliseconds. After timeout, the request is repeated according to **Retries** or the next configured RADIUS server is requested. Possible values are whole numbers between *50* and *50000*. The default value is *1000* (1 second).
Alive Check	Here you can activate a check of the reachability of a RADIUS server in **Status** *Down*. An Alive Check is carried out regularly (every 20 seconds) by sending an ACCESS_REQUEST to the IP address of the RADIUS server. If the server is reachable, **Status** is set to *alive* again. If the RADIUS server is only reachable over a switched line (dialup connection), this can cause additional costs if the server is *down* for a long time. The function is activated by choosing *Enabled*. The function is enabled by default.
Retries	Enter the number of retries for cases when there is no response to a request. If an answer has still not been received after these attempts, the **Status** is set to *down*. If the **Active Check** = *Enabled*your device tries to reach the server every 20 seconds. If the server answers, the **Status** is set back to *alive*. Possible values are whole numbers between *0* and *10*. The default value is *1*. To prevent **Status** being set to *down*, set this value to *0*.
RADIUS Dialout	Only for **Authentication Type** = *Authentication* and *IPSec Authentication*. Select whether your device receives requests from RADIUS server dialout routes. This enables temporary interfaces to be configured automatically and your device can initiate outgoing connections that are not configured permanently. The function is activated by choosing *Enabled*. The function is disabled by default.

Field	Value
	If the function is active, you can enter the following options: • *Reload Interval* Enter the time period in seconds between the update intervals. The default entry here is *0* i.e. an automatic reload is not carried out. • *Default User Password*: Some Radius servers require a user password for each RADIUS request. Enter the password that your device sends as the default user password in the prompt for the dialout routes on the RADIUS server.

9.5.2 TACACS+

TACACS+ permits access control for your device, network access servers (NAS) and other network components via one or more central servers.

Like RADIUS, TACACS+ is an AAA protocol and offers authentication, authorisation and accounting services (TACACS+ Accounting is currently not supported by **bintec** devices).

The following TACACS+ functions are available on your device:

- Authentication for login shell
- Command authorisation on the shell (e.g. telnet, show)

TACACS+ uses TCP port 49 and establishes a secure and encrypted connection.

In the **System Management** -> **Remote Authentication** -> **TACACS+** menu, a list of all registered TACACS+ servers is displayed.

9.5.2.1 Edit/New

Choose the icon to edit existing entries. Choose the **New** button to add TACACS+ servers.

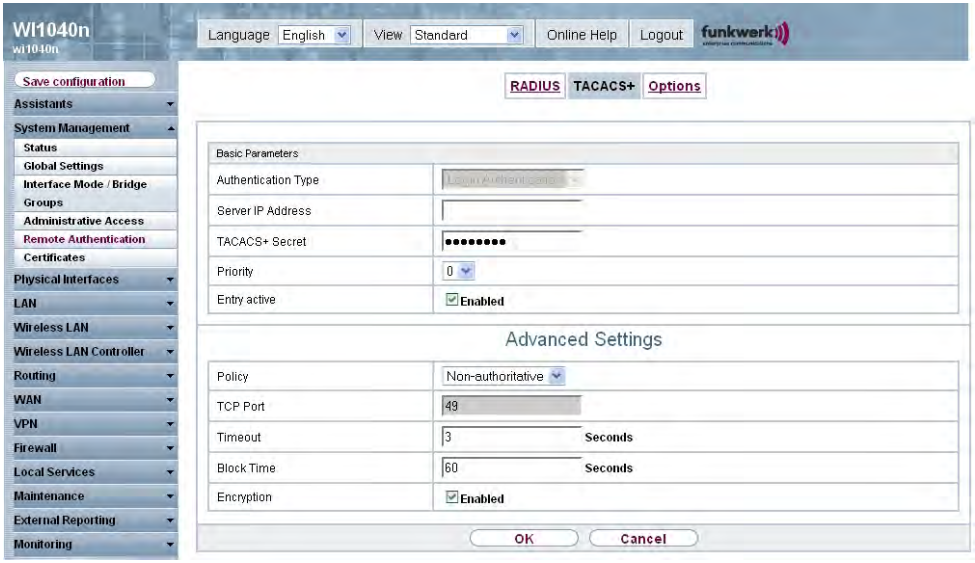


Fig. 44: **System Management** -> **Remote Authentication** -> **TACACS+** -> **New**

The **System Management** -> **Remote Authentication** -> **TACACS+** -> **New** menu consists of the following fields:

Fields in the TACACS+ Basic Parameters menu

Field	Description
Authentication Type	Displays which TACACS+ function is to be used. The value cannot be changed. Possible values: • `Login Authentication`: Here, you can define whether the current TACACS+ server is to be used for login authentication to your device.
Server IP Address	Enter the IP address of the TACACS+ server that is to be requested for login authentication.
TACACS+ Secret	Enter the password to be used to authenticate and, if applicable, encrypt data exchange between the TACACS+ server and the network access server (your device). The maximum length of the entry is 32 characters.
Priority	Assign a priority to the current TACACS+ server. The server with the lowest value is the one used first for TACACS+ login authentication. If this does not respond or access is denied (only if **Policy** = `Non-authoritative`), the entry with the

Field	Description
	next-highest priority is used. The available values are *0* to *9*, the default value is *0*.
Entry active	Select whether this server is to be used for login authentication. The function is activated by choosing *Enabled*. The function is enabled by default.

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Policy	Select the interpretation of the TACACS+ response. Possible values: • *Non-authoritative* (default value): The TACACS+ servers are queried in order of their priority (see **Priority**) until a positive response is received or a negative response is received from an authoritative server. • *Authoritative* : A negative response to a request is accepted, i.e. a request is not sent to another TACACS+ server. The device's internal user administration is is not turned off by TACACS+. It is checked after all TACACS+ servers have been queried.
TCP Port	Shows the default TCP port (*49*) used for the TACACS+ protocol. The value cannot be changed.
Timeout	Enter time in seconds for which the NAS is to wait for a response from TACACS+. If a response is not received during the wait time, the next configured TACACS+ server is queried (only if **Policy** = *Non-authoritative*) and the current server is set to status *Blocked*. The possible values are *1* to *60*, the default value is *3*.
Block Time	Enter the time in seconds for which the current server is to remain in blocked status.

Field	Description
	At the end of the block time, the server is set to the status specified in the **Administrative Status** field. The possible values are *0* to *3600*, the default value is *60*. The value *0* means that the server is never set to *Blocked* status and thus no other servers are queried.
Encryption	Select whether data exchange between the TACACS+ server and the NAS is to be encrypted with MD5. The function is activated by choosing *Enabled*. The function is enabled by default. If the function is not enabled, the packets and all related information are transferred unencrypted. Unencrypted transfer is not recommended as a default setting and should only be used for debugging.

9.5.3 Options

This setting possible here causes your device to carry out authentication negotiation for incoming calls, if it cannot identify the calling party number (e.g. because the remote terminal does not signal the calling party number). If the data (password, partner PPP ID) obtained by executing the authentication protocol is the same as the data of a listed remote terminal or RADIUS user, your device accepts the incoming call.

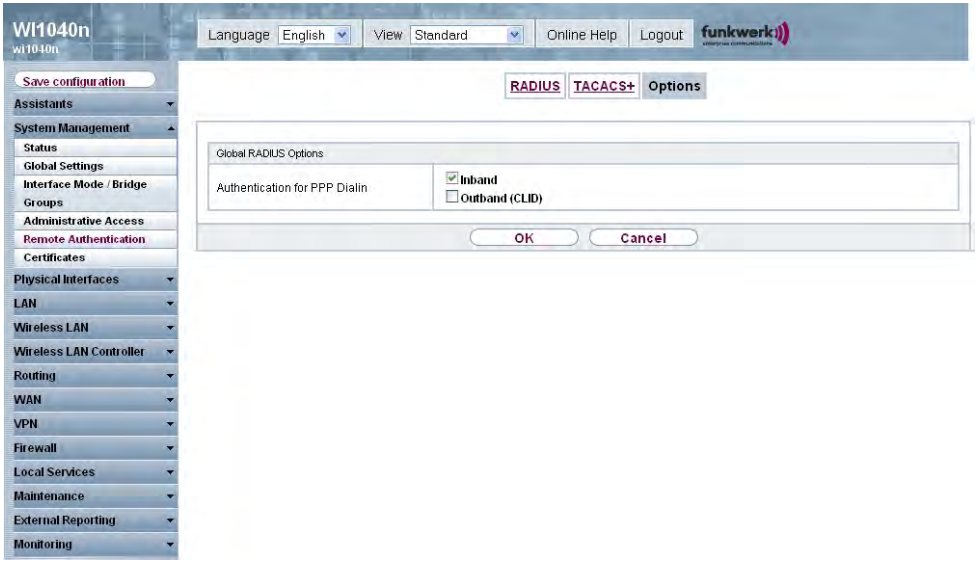


Fig. 45: **System Management** -> **Remote Authentication** -> **Options**

The **System Management** -> **Remote Authentication** -> **Options** menu consists of the following fields:

Fields in the Options Global RADIUS Options menu

Field	Description
Authentication for PPP Dialin	By default, the following authentication sequence is used for incoming calls with RADIUS: First CLID, then PPP and then PPP with RADIUS. Options: • *Inband* : Only inband RADIUS requests (PAP,CHAP, MS-CHAP V1 & V2) (i.e. PPP requests without CLID) are sent to the RADIUS server defined in **Server IP Address**. • *Outband (CLID)* : Only outband RADIUS requests (i.e. requests for calling line identification, CLID) are sent to the RADIUS server. *Inband* is activated by default.

9.6 Certificates

An asymmetric cryptosystem is used to encrypt data to be transported in a network, to generate or check digital signatures and the authenticate users. A key pair consisting of a public key and a private key is used to encrypt and decrypt the data.

For encryption the sender requires the public key of the recipient. The recipient decrypts the data using his private key. To ensure that the public key is the real key of the recipient and is not a forgery, a so-called digital certificate is required.

This confirms the authenticity and the owner of a public key. It is similar to an official passport in that it confirms that the holder of the passport has certain characteristics, such as gender and age, and that the signature on the passport is authentic. As there is more than one certificate issuer, e.g. the passport office for a passport, and as such certificates can be issued by several different issuers and in varying qualities, the trustworthiness of the issuer is extremely important. The quality of a certificate is regulated by the German Signature Act or respective EU Directives.

Certification authorities that issue so-called qualified certificates are organised in a hierarchy with the Federal Network Agency as the higher certifying authority. The structure and content of a certificate are stipulated by the standard used. X.509 is the most important and the most commonly use standard for digital certificates. Qualified certificates are personal and extremely trustworthy.

Digital certificates are part of a so-called Public Key Infrastructure (PKI). PKI refers to a system that can issue, distribute and check digital certificates.

Certificates are issued for a specific period, usually one year, i.e. they have a limited validity period.

Your device is designed to use certificates for VPN connections and for voice connections over Voice over IP.

9.6.1 Certificate List

In the **System Management** -> **Certificates** -> **Certificate List** menu a list of all available certificates is shown.

9.6.1.1 Edit

Click the icon to display the content of the selected object (key, certificate, or request).

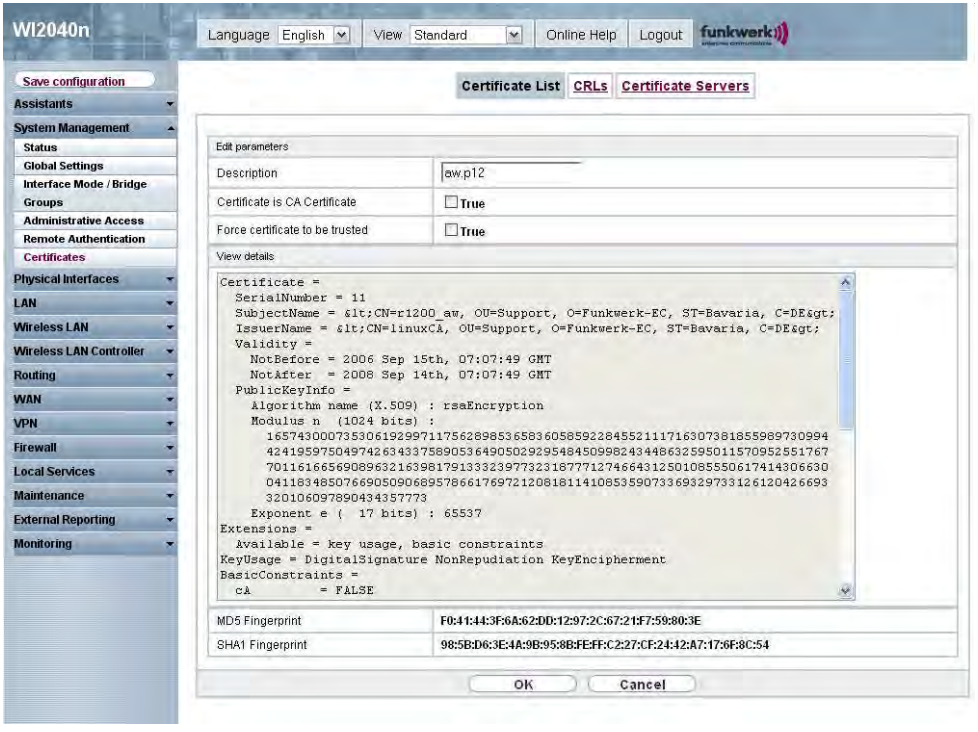


Fig. 46: **System Management** -> **Certificates** -> **Certificate List**->

The certificates and keys themselves cannot be changed, but a few external attributes can be changed, depending on the type of the selected entry.

The **System Management** -> **Certificates** -> **Certificate List**-> menu consists of the following fields:

Fields in the menu

Field	Description
Description	Shows the name of the certificate, key, or request.
Certificate is CA Certificate	Mark the certificate as a certificate from a trustworthy certification authority (CA). Certificates issued by this CA are accepted during authentication (unless specified otherwise under "Phase-1 Profiles"). The function is activated with `True`. The function is disabled by default.

Field	Description
Certificate Revocation List (CRL) Checking	Only for **Certificate is a CA certificate** = *True*. Define the extent to which certificate revocation lists (CRLs) are to be included in the validation of certificates issued by the owner of this certificate. Possible settings: • *Disabled* : No checking of CRLs. • *Always*: CRLs are always checked. • *Only if a CRL Distribution Point is present* (default value): If the CA certificate contains a CRL Distribution Point (CDP), this one is to be checked additionally to the revocation lists globally configured on the device. Under "View Details" in the certificate content you can check whether the CA certificate contains a CDP. • *Use Settings from superior certificate*: The settings of the higher level certificate are used, if one exists. It is does not, the same procedure is used as that described under "Only if a CRL Distribution Point is present".
Force certificate to be trusted	Define that this certificate is to be accepted as the user certificate without further checks during authentication. The function is activated with *True*. The function is disabled by default.

Caution

It is extremely important for VPN security that the integrity of all certificates manually marked as trustworthy (certification authority and user certificates) is ensured. The displayed "fingerprints" can be used to check this integrity: Compare the displayed values with the fingerprints specified by the issuer of the certificate (e.g. on the Internet). It is sufficient to check one of the two values.

9.6.1.2 Request

Registration authority certificates in SCEP

If SCEP is used, your device also supports separate registration authority certificates.

Registration authority certificates are used by some Certificate Authorities (CAs) to handle certain tasks (signature and encryption) during SCEP communication with separate keys, and to delegate the operation to separate registration authorities, if applicable.

When a certificate is downloaded automatically, i.e. if **CA Certificates** = *-Download-* is selected, all the certificates needed for the operation are loaded automatically.

If all the necessary certificates are already available in the system, these can also be selected manually.

Select the **Request** button to request or import more certificates.

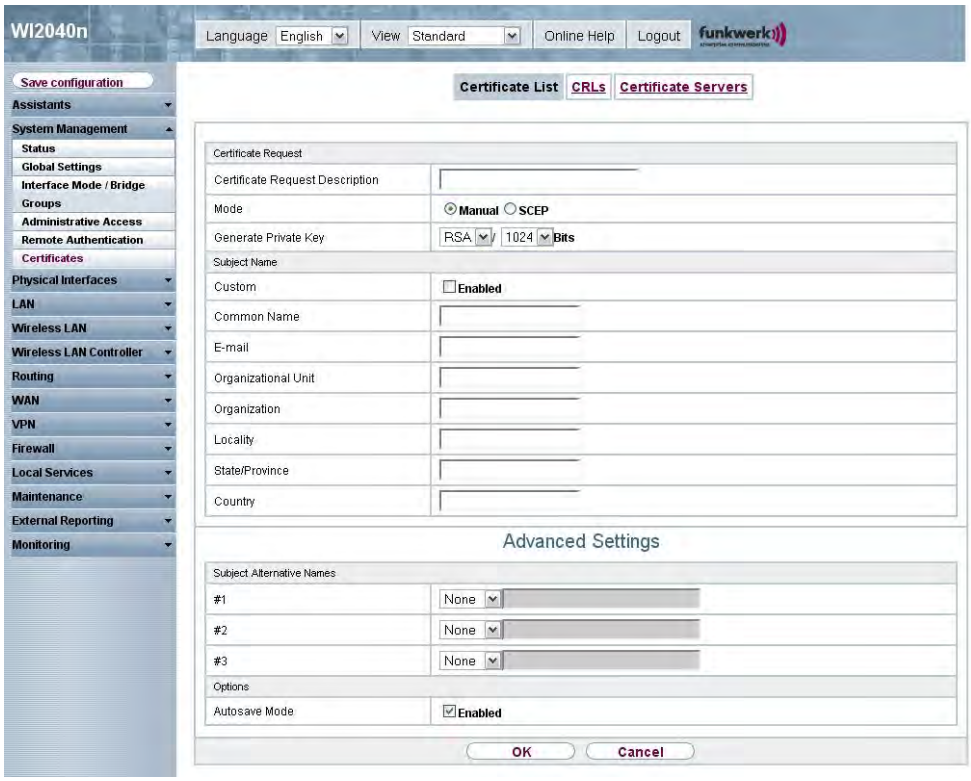


Fig. 47: **System Management** ->**Certificates** -> **Certificate List** -> **Request**

The **System Management** -> **Certificates** -> **Certificate List** -> **Request** menu consists of the following fields:

Fields in the Certificate List Certificate Request menu

Field	Description
Certificate Request De-	Enter a unique description for the certificate.

Field	Description
scription	
Mode	Select the way in which you want to request the certificate. Possible settings: • *Manual* (default value): Your device generates a PKCS#10 for the key. This file can then be uploaded directly in the browser or copied in the **Edit** menu using the **View Details** field. This file must be provided to the CA and the received certificate must then be imported manually to your device. • *SCEP*: The key is requested from a CA using the Simple Certificate Enrolment Protocol.
Generate Private Key	Only if **Mode** = *Manual*. Select an algorithm for key creation. *RSA* (default value) and *DSA* are available. Also select the length of the key to be created. Possible values: *512*, *768*, *1024*, *1536*, *2048*, *4096*. Please note that a key with a length of 512 bits could be rated as unsecure, whereas a key of 4096 bits not only needs a lot of time to create, but also occupies a major share of the resources during IPSec processing. A value of 768 or more is, however, recommended and the default value is 1024 bits.
SCEP URL	Only if **Mode** = *SCEP*. Enter the URL of the SCEP server, e.g. http://scep.funkwerk.de:8080/scep/scep.dll Your CA administrator can provide you with the necessary data.
CA Certificate	Only if **Mode** = *SCEP*. Select the CA certificate. • *-Download-*: In **CA Name**, enter the name of the CA certificate of the certification authority (CA) from which you wish to request your certificate, e.g. *cawindows*. Your CA adminis-

Field	Description
	trator can provide you with the necessary data. If no CA certificates are available, the device will first download the CA certificate of the relevant CA. It then continues with the enrolment process, provided no more important parameters are missing. In this case, it returns to the **Generate Certificate Request** menu. If the CA certificate does not contain a CRL distribution point (Certificate Revocation List, CRL), and a certificate server is not configured on the device, the validity of certificates from this CA is not checked. • <name of an existing certificate>: If all the necessary certificates are already available in the system, you select these manually.
RA Sign Certificate	Only if **Mode** = *SCEP*. Only if **CA Certificates** is not = *-Download-*. Select a certificate for signing SCEP communication. The default value is *-Use CA Certificate-*, i.e. the CA certificate is used.
RA Encrypt Certificate	Only if **Mode** = *SCEP*. Only if **RA Sign Certificate** is not = *-Use CA Certificate-*. If you use one of your own certificates to sign communication with the RA, you can select another one here to encrypt communication. The default value is *-Use RA Sign Certificate-*, i.e. the same certificate is used as for signing.
Password	Only if **Mode** = *SCEP*. You may need a password from the certification authority to obtain certificates for your keys. Enter the password you received from the certification authority here.

Fields in the Certificate List Subject Name menu

Field	Description
Custom	Select whether you want to enter the name components of the subject name individually as specified by the CA or want to enter a special subject name. If *Enabled* is selected, a subject name can be given in **Summary** with attributes that are not offered in the list. Example: "CN=VPNServer, DC=mydomain, DC=com, c=DE". If the field is not marked, enter the name components in **Common Name**, **E-mail**, **Organisational Unit**, **Organisation**, **Location**, **State/Province** and **Country**. The function is disabled by default.
Summary	Only for **Custom** = enabled. Enter a subject name with attributes not offered in the list. Example: "CN=VPNServer, DC=mydomain, DC=com, c=DE".
Common Name	Only for **Custom** = disabled. Enter the name according to CA.
E-mail	Only for **Custom** = disabled. Enter the e-mail address according to CA.
Organisational Unit	Only for **Custom** = disabled. Enter the organisational unit according to CA.
Organisation	Only for **Custom** = disabled. Enter the organisation according to CA.
Locality	Only for **Custom** = disabled. Enter the location according to CA.
State/Province	Only for **Custom** = disabled. Enter the state/province according to CA.
Country	Only for **Custom** = disabled.

Field	Description
	Enter the country according to CA.

The **Advanced Settings** menu consists of the following fields:

Fields in the Advanced Settings Subject Alternative Names menu

Field	Description
#1, #2, #3	For each entry, define the type of name and enter additional subject names. Possible values: • *None* (default value): No additional name is entered. • *IP*: An IP address is entered. • *DNS*: A DNS name is entered. • *Email*: An e-mail address is entered. • *URI*: A uniform resource identifier is entered. • *DN*: A distinguished name (DN) name is entered. • *RID*: A registered identity (RID) is entered.

Fields in the Advanced Settings Options menu

Field	Description
Autosave Mode	Select whether your device automatically stores the various steps of the enrolment internally. This is an advantage if enrolment cannot be concluded immediately. If the status has not been saved, the incomplete registration cannot be completed. As soon as the enrolment is completed and the certificate has been downloaded from the CA server, it is automatically saved in the device configuration. The function is activated with *Enabled*. The function is enabled by default.

9.6.1.3 Import

Choose the **Import** button to import other certificates.

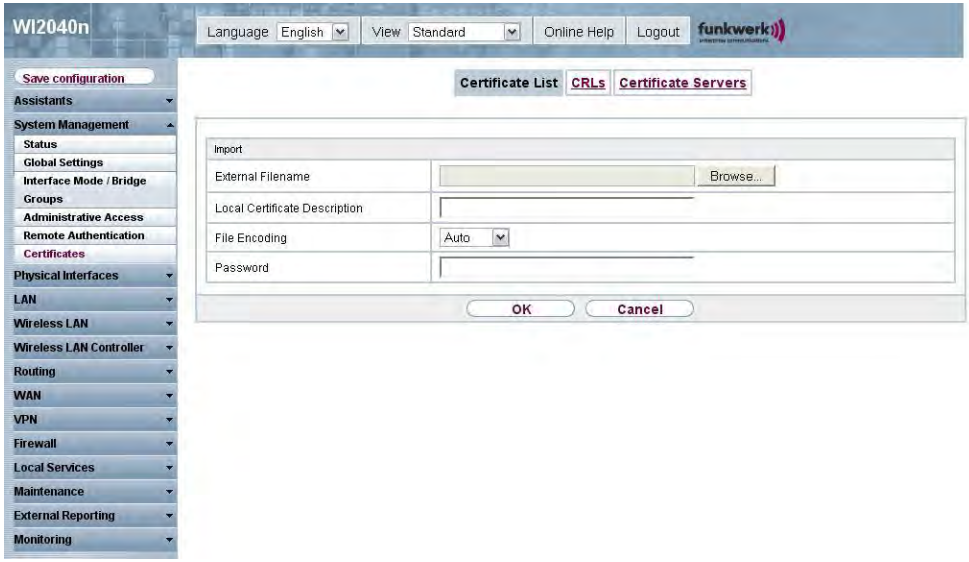


Fig. 48: **System Management** -> **Certificates** -> **Certificate List** -> **Import**

The **System Management** -> **Certificates** -> **Certificate List** -> **Import** menu consists of the following fields:

Fields in the Certificate List Import menu

Field	Description
External Filename	Enter the file path and name of the certificate to be imported, or use **Browse...** to select it from the file browser.
Local Certificate Description	Enter a unique description for the certificate.
File Encoding	Select the type of coding so that your device can decode the certificate. Possible values: • *auto* (default value) Activates automatic code recognition. If downloading the certificate in auto mode fails, try with a certain type of encoding. • *Base64* • *Binary*
Password	You may need a password to obtain certificates for your keys.

Field	Description
	Enter the password here.

9.6.2 CRLs

In the **System Management** -> **Certificates** -> **CRLs** menu a list of all CRLs is shown.

If a key is no longer to be used, e.g. because it has fallen into the wrong hands or has been lost, the corresponding certificate is declared invalid. The certification authority revokes the certificate and publishes it on a certificate blacklist, so-called CRL. Certificate users should always check against these lists to ensure that the certificate used is currently valid. This check can be automated via a browser.

The Simple Certificate Enrollment Protocol (SCEP) supports the issue and revocation of certificates in networks.

9.6.2.1 Import

Choose the **Import** button to import other CRLs.

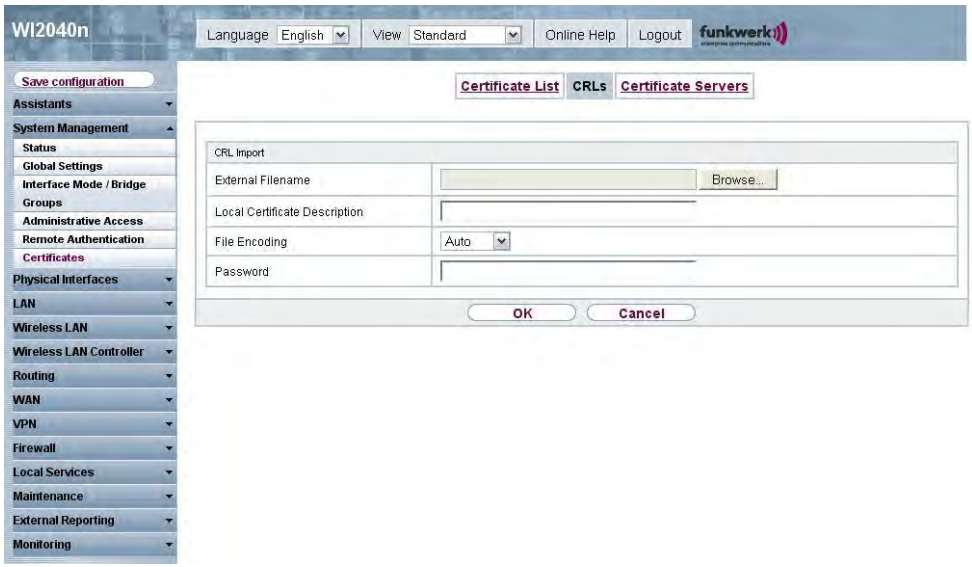


Fig. 49: **System Management** -> **Certificates** -> **CRLs** -> **Import**

The **System Management** -> **Certificates** -> **CRLs** -> **Import** menu consists of the following fields:

Fields in the CRLs CRL Import menu

Field	Description
External Filename	Enter the file path and name of the CRL to be imported, or use **Browse...** to select it from the file browser.
Local Certificate Description	Enter a unique description for the CRL.
File Encoding	Select the type of encoding, so that your device can decode the CRL. Possible values: • *auto* (default value) Activates automatic code recognition. If downloading the CRL in auto mode fails, try with a certain type of encoding. • *Base64* • *Binary*
Password	Enter the password to be used for the import.

9.6.3 Certificate Servers

In the **System Management** -> **Certificates** -> **Certificate Servers** menu a list of all certificate servers is shown.

A certificate server provides for certificate revocation lists (CRL), that are used by the device to verify certificates via LDAP or HTTP.

9.6.3.1 New

Choose the **New** button to set up new certificate servers.

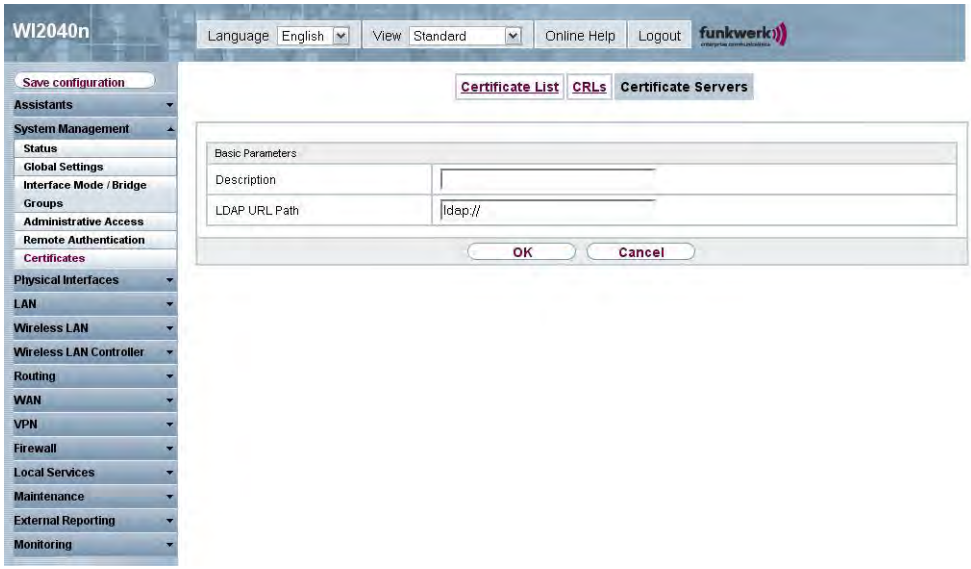


Fig. 50: **System Management** -> **Certificates** -> **Certificate Servers** -> **New**

The **System Management** -> **Certificates** -> **Certificate Servers** -> **New** menu consists of the following fields:

Fields in the Certificate Servers Basic Parameters menu

Field	Description
Description	Enter a unique description for the certificate server.
LDAP URL Path	Enter the LDAP URL of the server.

Chapter 10 Physical Interfaces

In this menu, you configure the physical interfaces that you have used when connecting your gateway. The configuration interface only shows the interfaces that are available on your device. In the **System Management** -> **Status** menu you can see a list of all physical interfaces and information on whether the interfaces are connected or active and whether they have already been configured.

10.1 Ethernet Ports

An Ethernet interface is a physical interface for connection to the local network or external networks.

Note

In the ex works state, the Ethernet ports ETH1 and ETH2 are assigned to the standard bridge group `br0`, which is configured as DHCP client and with the fallback **IP address** `192.168.0.252` and **Netmask** `255.255.255.0`.

10.1.1 Port Configuration

Your device allows you to configure the two Ethernet interfaces separately.

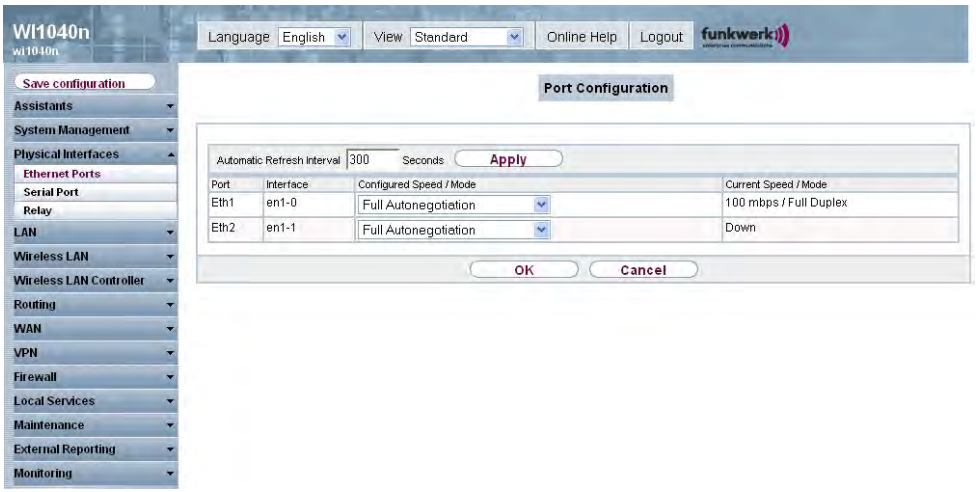


Fig. 51: **Physical Interfaces** -> **Ethernet Ports** -> **Port Configuration**

The **Physical Interfaces** -> **Ethernet Ports** -> **Port Configuration** menu consists of the following fields:

Fields in menu Port Configuration

Field	Description
Port	Shows the respective port. The numbering corresponds to the numbering of the Ethernet ports on the back of the device.
Interface	Displays the interface assigned to the Ethernet port here.
Configured Speed / Mode	Select the mode in which the interface is to run. Possible values: • *Full Autonegotiation* (default value) • *Auto 100 mbps only* • *Auto 10 mbps only* • *Auto 100 mbps / Full Duplex* • *Auto 100 mbps / Half Duplex* • *Auto 10 mbps / Full Duplex* • *Auto 10 mbps / Half Duplex* • *Fixed 100 mbps / Full Duplex* • *Fixed 100 mbps / Half Duplex* • *Fixed 10 mbps / Full Duplex* • *Fixed 10 mbps / Half Duplex* • *Disabled*: The interface is created but remains inactive.
Current Speed / Mode	Shows the actual mode and actual speed of the interface. Possible values: • *100 mbps / Full Duplex* • *100 mbps / Half Duplex* • *10 mbps / Full Duplex* • *10 mbps / Half Duplex* • *Inactive*

10.2 Serial Port

The serial interface can be operated as a console or as a data interface. In data interface mode, the data for the serial interface can be transmitted over an IP infrastructure (Serial over IP).

10.2.1 Serial Port

You can make settings for the serial interface in the **Physical Interfaces** -> **Serial Port** -> **Serial Port** menu.

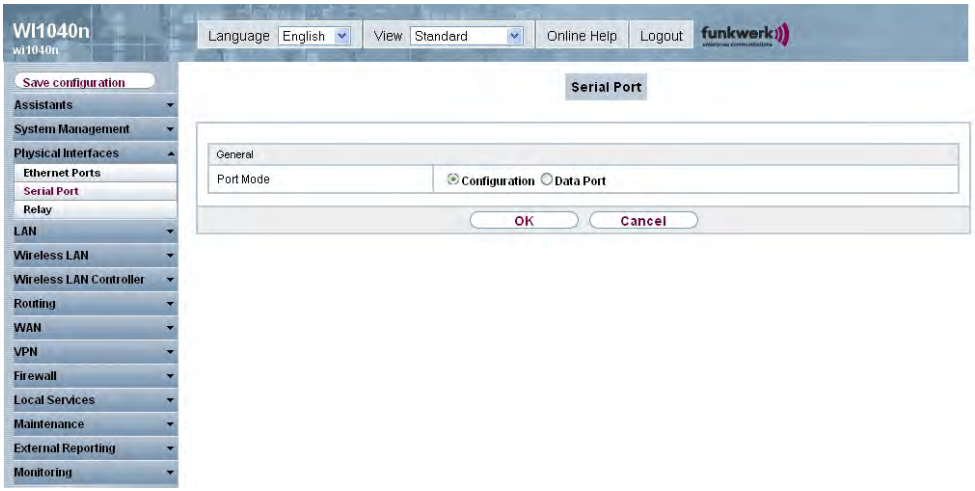


Fig. 52: **Physical Interfaces** -> **Serial Port** -> **Serial Port**

The **Physical Interfaces** -> **Serial Port** -> **Serial Port** menu consists of the following fields:

Fields in the Serial Port General menu

Field	Description
Port Mode	Select in which mode the serial interface is to be used. Possible values: • `Configuration` (default value): The serial interface is used as a console. • `Data Port`: The serial interface is operated as a data interface, Serial over IP is used.

If the *Data Port* option is selected for the **Port Mode**, an extra configuration section opens.

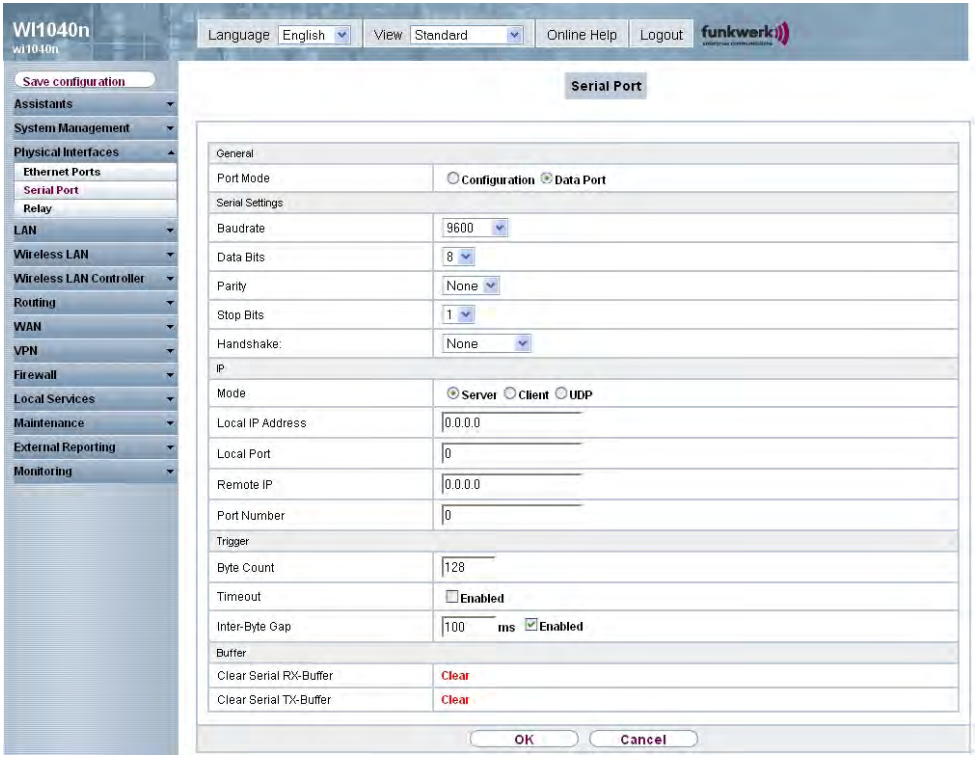


Fig. 53: **Physical Interfaces** -> **Serial Port** -> **Serial Port** *with* **Port Mode** = *Data Port*

Fields in the Serial Port Serial Settings menu

Field	Description
Baudrate	Select which baud rate should be used. Make sure that the remote terminal is suitable for the selected baud rate. If this is not the case, you will not be able to establish a serial connection to the device. Possible values: • *300* • *600* • *1200* • *2400* • *4800*

Field	Description
	• *9600* (default value) • *19200* • *57600* • *115200*
Data Bits	Select how many data bits should be sent in sequence for traffic data. Possible values: • *8* (default value): Eight data bits are sent in sequence. • *7*: Seven data bits are sent in sequence.
Parity	Select whether or not a parity bit should be used to identify transmission errors. Possible values: • *None* (default value): No parity bit is used. • *Even*: An even number of "1" bits is used to identify transmission errors. • *Uneven*: An uneven number of "1" bits is used to identify transmission errors.
Stop Bits	Stop bits terminate the data transmission of a transmission unit. Choose whether a stop bit should be used or whether two stop bits should be used. Possible values: • *1* (default value) • *2*
Handshake	Only for **Port Mode** = *Data Port* Choose how the recipient can continue the data transmission so that no data is lost, if no other data can be processed. Possible values: • *None* (default value): The recipient is unable to continue the data transmission.

Field	Description
	• *RTS/CTS*: The hardware handshake used controls the data flow over the RTS and CTS lines. • *XON/XOFF*: If the software handshake is used, the recipient sends special signs to the sender to control the data flow.

Fields in the Serial Port IP menu

Field	Description
Mode	Select the mode in which the gateway should process IP data packets. Possible values: • *Server* (default value): The gateway waits for incoming TCP connections. • *Client*: The gateway actively sets up a TCP connection. • *UDP*: The gateway sends and receives UDP packets.
Local IP Address	Enter the IP address of the client logging in. If **Local IP Address** = *0.0.0.0*, any client can log in.
Local Port	Enter the port for the **Local IP Address**.
Remote IP	Enter the IP address of the server at which your gateway should log in.
Port Number	Enter the port for the **Remote IP**.

Fields in the Serial Port Trigger menu

Field	Description
Byte Count	Enter the received characters in bytes, which are used as a trigger for data transmission. The function is activated with *Enabled*. The function is enabled by default. Possible values: *1* .. *1460*. Default value: *128*.
Timeout	Enter the time in ms since receiving the last character, which is used as a trigger for data transmission. The function is activated with *Enabled*.

Field	Description
	The function is enabled by default. Possible values: *0* .. *65535*. Default value: *0*.
Inter-Byte Gap	Enter the time in ms since receiving the first character, which is used as a trigger for data transmission. The function is activated with *Enabled*. The function is disabled by default. Possible values: *0* .. *65535*. Default value: *100*.

Fields in the Serial Port Buffer menu

Field	Description
Clear Serial RX-Buffer	Click the **Clear** button to clear the receive buffer.
Clear Serial TX-Buffer	Click the **Clear** button to clear the send buffer.

10.3 Relay

Devices of the **WI series** are fitted with a relay. The rest (i.e. normal/unexcited/fault) state of the contacts is open. You can choose whether the relay is manually controlled or used as an alarm relay, coupled with the red error LED. When manually controlled, the state of the relay is set during booting when the configuration is loaded.

10.3.1 Relay Configuration

In this menu, you can configure the port mode.

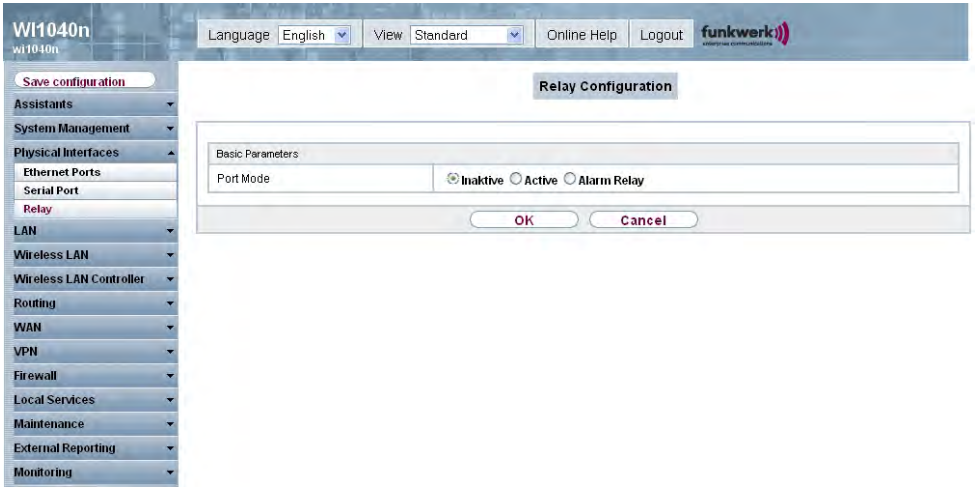


Fig. 54: **Physical Interfaces** -> **Relay** -> **Relay Configuration**

The **Physical Interfaces** -> **Relay** -> **Relay Configuration** menu consists of the following fields:

Fields in the Relay Configuration Basic Parameters menu

Field	Description
Port Mode	Possible values: • *Inactive* (default value): The relay is manually set to always open. • *Active*: The relay is manually set to always closed. • *Alarm relay*: The relay is automatically coupled with the red error LED.

Chapter 11 LAN

In this menu, you configure the addresses in your LAN and can structure your local network using VLANs.

11.1 IP Configuration

In this menu, you can edit the IP configuration of the LAN and Ethernet interfaces of your device.

11.1.1 Interfaces

In the **LAN** -> **IP Configuration** -> **Interfaces** menu, the available IP interfaces are listed. You can edit the IP configuration of the interfaces or create virtual interfaces for special applications. Here is a list of all of the interfaces (logical Ethernet interfaces and others created in the subsystems) configured in the **System Management**-> **Interface Mode / Bridge Groups** -> **Interfaces** menu.

Use the to edit the settings of an existing interface (bridge groups, Ethernet interfaces in routing mode).

You can use the **New** button to create virtual interfaces. However, this is only needed in special applications (e.g. BRRP).

Depending on the option selected, different fields and options are available. All the configuration options are listed below.

The default setting for all existing interfaces of your device is Bridging mode. In the ex works state the bridge group **br0** is pre-configured as a DHCP client with the fallback IP address *192.168.0.252* and netmask *255.255.255.0*.

Note

Please note:

If your device has obtained an IP address dynamically from a DHCP server operated in your network for the basic configuration, the fallback IP address 192.168.0.252 is deleted automatically and your device will no longer function over this address.

However, if you have set up a connection to the device over the fallback IP address 192.168.0.252 or have assigned an IP address with the **Dime Manager** in the basic

configuration, you will only be able to access your device over this IP address. The device will no longer obtain an IP configuration dynamically over DHCP.

Example of subnets

If your device is connected to a LAN that consists of two subnets, you should enter a second **IP Address/Netmask**.

The first subnet has two hosts with the IP addresses 192.168.42.1 and 192.168.42.2, for example, and the second subnet has two hosts with the IP addresses 192.168.46.1 and 192.168.46.2. To be able to exchange data packets with the first subnet, your device uses the IP address 192.168.42.3, for example, and 192.168.46.3 for the second subnet. The netmasks for both subnets must also be indicated.

11.1.1.1 Edit/New

Choose the icon to edit existing entries. Choose the **New** button to create virtual interfaces.

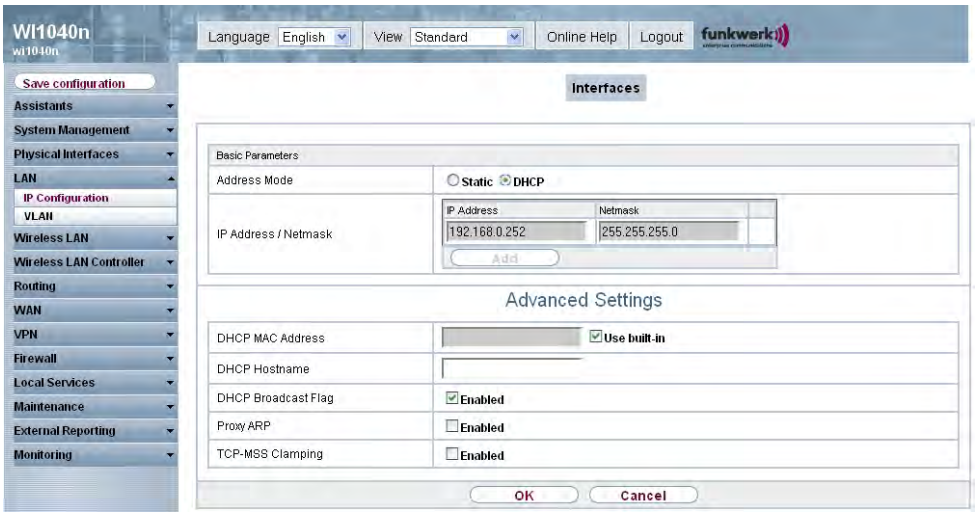


Fig. 55: **LAN** -> **IP Configuration** -> **Interfaces** -> **Edit/New**

The **LAN** -> **IP Configuration** -> **Interfaces** -> **Edit/New** menu consists of the following fields:

Fields in the Interfaces Basic Parameters menu

Field	Description
Based on Ethernet Interface	This field is only displayed if you are editing a virtual routing interface. Select the Ethernet interface for which the virtual interface is to be configured.
Address Mode	Select how an IP address is assigned to the interface. Possible values: • *Static* (default value): A static IP address is assigned to the interface in **IP Address/Netmask**. • *DHCP*: An IP address is assigned to the interface dynamically via DHCP.
IP Address/Netmask	Only if **Address Mode** = *Static* With **Add**, add a new adress entry and enter the **IP Address** and corresponding **Netmask**
Interface Mode	Only for physical interfaces in routing mode. Select the configuration mode of the interface. Possible values: • *Untagged* (default value): The interface is not assigned for a specific purpose. • *Tagged (VLAN)*: This option only applies for routing interfaces. You use this option to assign the interface to a VLAN. This is done using the VLAN ID, which is displayed in this mode and can be configured. In this mode, the definition of a MAC address in **MAC Address** is optional.
MAC Address	Only for virtual interfaces and if **Interface Mode** = *Untagged* Enter the MAC address associated with the interface. For virtual interfaces, you can use the MAC address of the physical interface under which the virtual interface was created, but this is not necessary. You can also allocate a virtual MAC address. The first 6 characters of the MAC are preset (but can be changed).

Field	Description
VLAN ID	Only if **Interface Mode** = *Tagged (VLAN)* This option only applies for routing interfaces. Assign the interface to a VLAN by entering the VLAN ID of the relevant VLAN. Possible values are *1* (default value) to *4094*.

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
DHCP MAC Address	Only if **Address Mode** = *DHCP* If **Use Built-In** is activated (default setting), the hardware MAC address of the Ethernet interface is used. In the case of physical interfaces, the current MAC address is entered by default. If you disable **Use Built-In**, you enter a MAC address for the virtual interface, e.g. *00:e1:f9:06:bf:03*. Some providers use hardware-independent MAC addresses to allocate their clients IP addresses dynamically. If your provider has assigned you a MAC address, enter this here.
DHCP Hostname	Only if **Address Mode** = *DHCP* Enter the host name requested by the provider. The maximum length of the entry is 45 characters.
DHCP Broadcast Flag	Only if **Address Mode** = *DHCP* Choose whether or not the BROADCAST bit is set in the DHCP requests for your device. Some DHCP servers that assign IP addresses by UNICAST do not respond to DHCP requests with the set BROADCAST bit. In this case, it is necessary to send DHCP requests in which this bit is not set. In this case, disable this option. The function is activated by choosing *Enabled*. The function is enabled by default.
Proxy ARP	Select whether your device is to respond to ARP requests from its own LAN on behalf of defined remote terminals.

Field	Description
	The function is activated by choosing *Enabled*. The function is disabled by default.
TCP-MSS Clamping	Select whether your device is to apply MSS Clamping. To prevent IP packets fragmenting, the MSS (Maximum Segment Size) is automatically decreased by the device to the value set here. The function is activated by choosing *Enabled*. The function is disabled by default. Once enabled, the default value *1350* is entered in the input field.

11.2 VLAN

By implementing VLAN segmentation in accordance with 802.1Q, you can configure VLANs on your device. The wireless ports of an access point, in particular, are able to remove the VLAN tag of a frame sent to the clients and to tag received frames with a predefined VLAN ID. This functionality makes an access point nothing less than a VLAN-aware switch with the enhancement of grouping clients into VLAN groups. In general, VLAN segmenting can be configured with all interfaces.

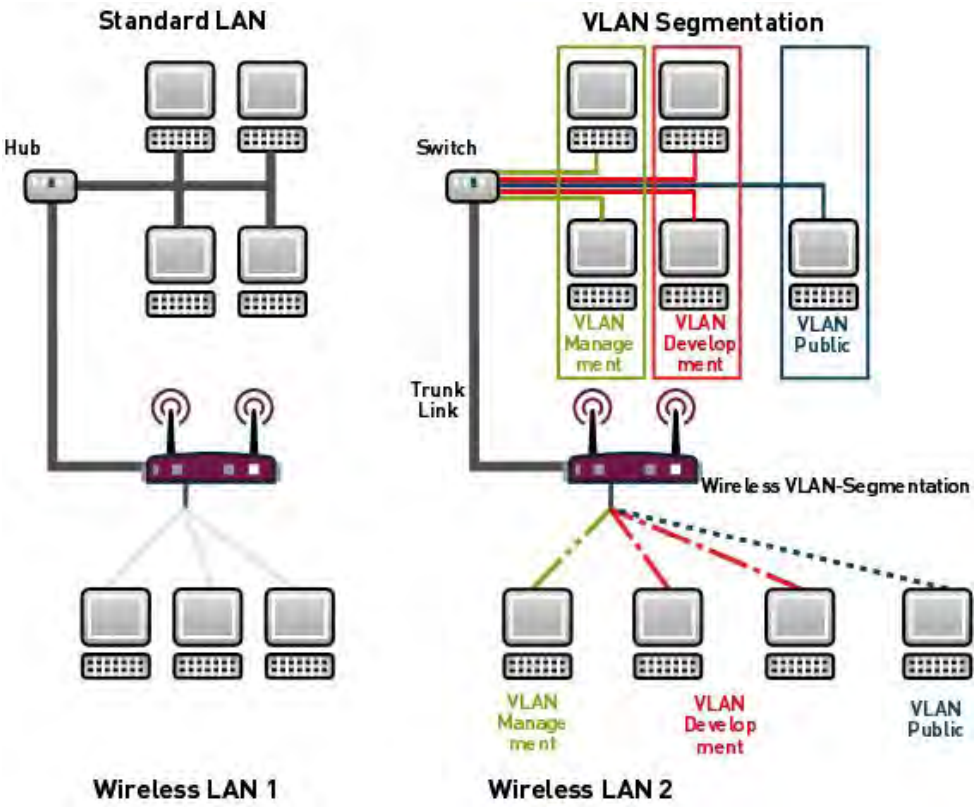


Fig. 56: VLAN segmenting

VLAN for Bridging and VLAN for Routing

In the **LAN** -> **VLAN** menu, VLANs (virtual LANs) are configured with interfaces that operate in bridging mode. Using the **VLAN** menu, you can make all the settings needed for this and query their status.

Caution

For interfaces that operate in Routing mode, you only assign a VLAN ID to the interface. You define this via the parameter **Interface Mode** = *VLAN* and the **VLAN ID** field in the **LAN** -> **IP Configuration** ->**Interfaces** -> **New** menu.

11.2.1 VLANs

In this menu, you can display all the VLANs already configured, edit your settings and create new VLANs. By default, the `Management` VLAN is available, to which all interfaces are assigned.

11.2.1.1 Edit/New

Choose the icon to edit existing entries. Choose the **New** button to configure other VLANs.

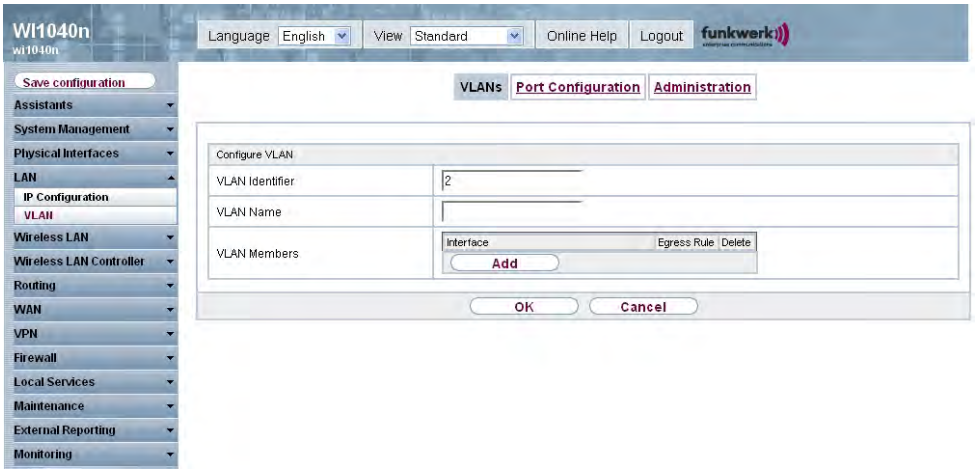


Fig. 57: **LAN** -> **VLAN** -> **VLANs** -> **Edit/New**

The **LAN** -> **VLAN** -> **VLANs** -> **Edit/New** menu consists of the following fields:

Fields in the VLANs Configure VLAN menu

Field	Description
VLAN Identifier	Enter the number that identifies the VLAN. In the **Edit** menu, you can no longer change this value. Possible values are `1` to `4094`.
VLAN Name	Enter a unique name for the VLAN. A character string of up to 32 characters is possible.
VLAN Members	Select the ports that are to belong to this VLAN. You can use the **Add** button to add members.

Field	Description
	For each entry, also select whether the frames to be transmitted from this port are to be transmitted `tagged` (i.e. with VLAN information) or `untagged` (i.e. without VLAN information).

11.2.2 Port Configuration

In this menu, you can define and view the rules for receiving frames at the VLAN ports.

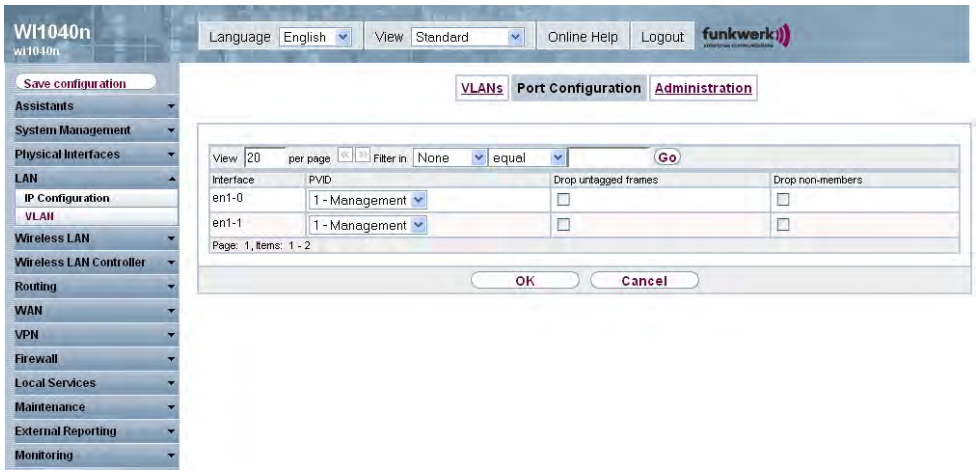


Fig. 58: **LAN -> VLAN -> Port Configuration**

The **LAN -> VLAN-> Port Configuration** menu consists of the following fields:

Fields in menu Port Configuration

Field	Description
Interface	Shows the port for which you define the PVID and processing rules.
PVID	Assign the selected port the required PVID (Port VLAN Identifier). If a packet without a VLAN tag reaches this port, it is assigned this PVID.
Drop untagged frames	If this option is enabled, untagged frames are discarded. If the option is disabled, untagged frames are tagged with the PVID defined in this menu.

Field	Description
Drop non-members	If this option is enabled, all tagged frames that are tagged with a VLAN ID to which the selected port does not belong are discarded.

11.2.3 Administration

In this menu, you make general settings for a VLAN. The options must be configured separately for each bridge group.

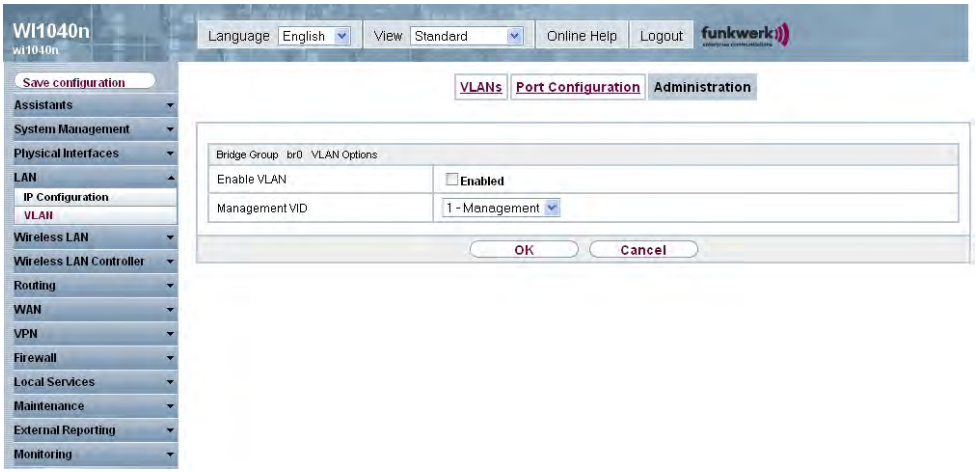


Fig. 59: **LAN -> VLAN -> Administration**

The **LAN -> VLAN -> Administration** menu consists of the following fields:

Fields in the Administration Bridge Group br<ID> VLAN Options menu

Field	Description
Enable VLAN	Enable or disable the specified bridge group for VLAN. The function is activated with `Enabled`. The function is not activated by default.
Management VID	Select the VLAN ID of the VLAN in which your device is to operate.

Chapter 12 Wireless LAN

In the case of wireless LAN (WLAN = Wireless Local Area Network), this relates to the creation of a network using wireless technology.

Network functions

Like a wired network, a WLAN offers all the main network functions. Access to servers, files, printers, and the e-mail system is just as reliable as company-wide Internet access. Because the devices do not require any cables, the great advantage of WLAN is that there are no building-related restrictions (i.e. the device location does not depend on the position and number of connections).

Currently applicable standard: IEEE 802.11

In the case of 802.11-WLANs, all the functions of a wired network are possible. WLAN transmits inside and outside buildings with a maximum of 100 mW.

IEEE 802.11g is currently the most widespread standard for wireless LANs and offers a maximum data transmission rate of 54 mbps. This procedure operates in the radio frequency range of 2.4 GHz, which ensures that parts of the building are penetrated as effectively as possible with a low transmission power that poses no health risks.

A 802.11g-compatible standard is 802.11b, which operates in the 2.4 GHz range (2400 MHz - 2485 MHz) and offers a maximum data transmission rate of 11 mbps. 802.11b and 802.11g WLAN systems involve no charge or login.

With 802.11a, bandwidths of up to 54 mbps can be used in the 5150 GHz to 5725 MHz range. With the higher frequency range, 19 non-overlapping frequencies are available (in Germany). This frequency range can also be used without a licence in Germany. In Europe, transmission power of not just 30 mW but 1000 mW can be used with 802.11h, but only if TPC (TX Power Control, method for controlling transmission power in wireless systems to reduce interferences) and DFS (Dynamic Frequency Selection) are used. The purpose of TPC and DFS is to ensure that satellite connections and radar devices are not interfered with.

The standard 802.11n (Draft 2.0) uses MIMO technology (Multiple Input Multiple Output) for data transmission that allows data transfer via WLAN over longer distances or with higher data rates. With bandwidth 20 MHz or 40 MHz a gross data rate of 150 Mbps or 300 Mbps is achieved.

An amendment to the Telecommunications Act (TKG) allowed the 5.8 GHz band (5755 MHz - 5875 MHz) to be used for so-called BFWA applications (Broadband Fixed Wireless Access). This simply requires registration with the Federal Network Agency. However, the use of TPC and DFS is mandatory in this case.

12.1 WLAN

In the **Wireless LAN** -> **WLANx** menu, you can configure all the WLAN modules of your device.

Depending on the model, one or more WLAN modules, **WLAN1** and, in certain models, **WLAN2** and **WLAN3**, are available.

12.1.1 Radio Settings

In the **Wireless LAN** -> **WLAN** -> **Radio Settings** menu, an overview of all the configuration options for the WLAN module is shown.

Fig. 60: **Wireless LAN -> WLAN -> Radio Settings**

12.1.1.1 Radio Settings -> Edit

In this menu, you change the settings for the wireless module.

Choose the button to edit the configuration.

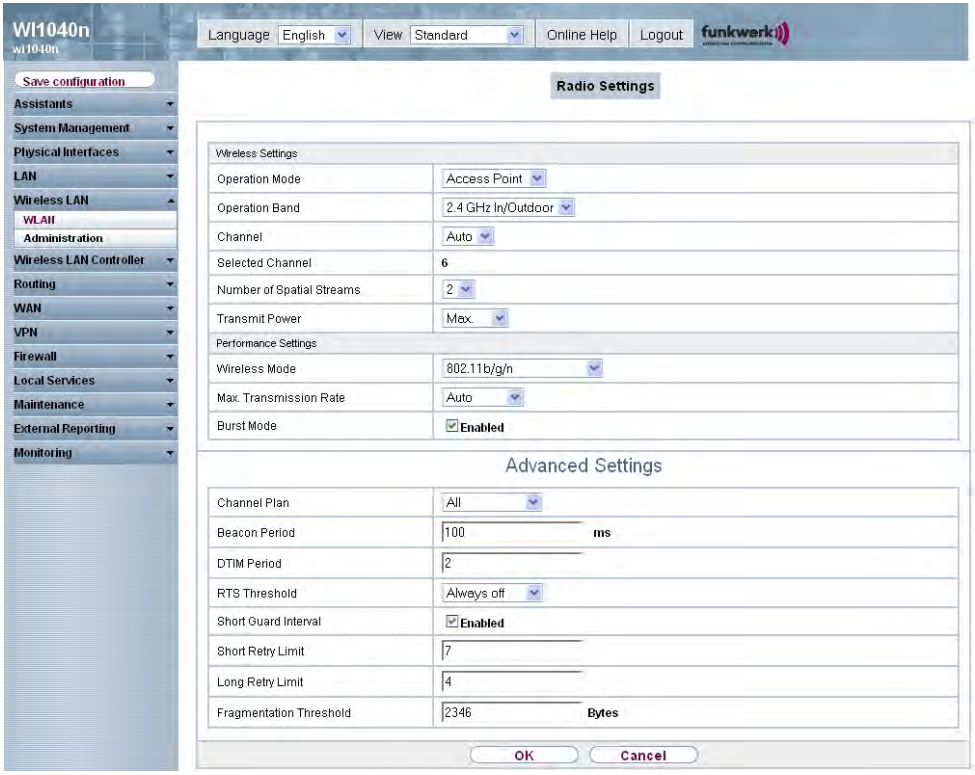


Fig. 61: **Wireless LAN** -> **WLAN** -> **Radio Settings** -> **Advanced Settings** *for* **Operation Mode** `Access Point`

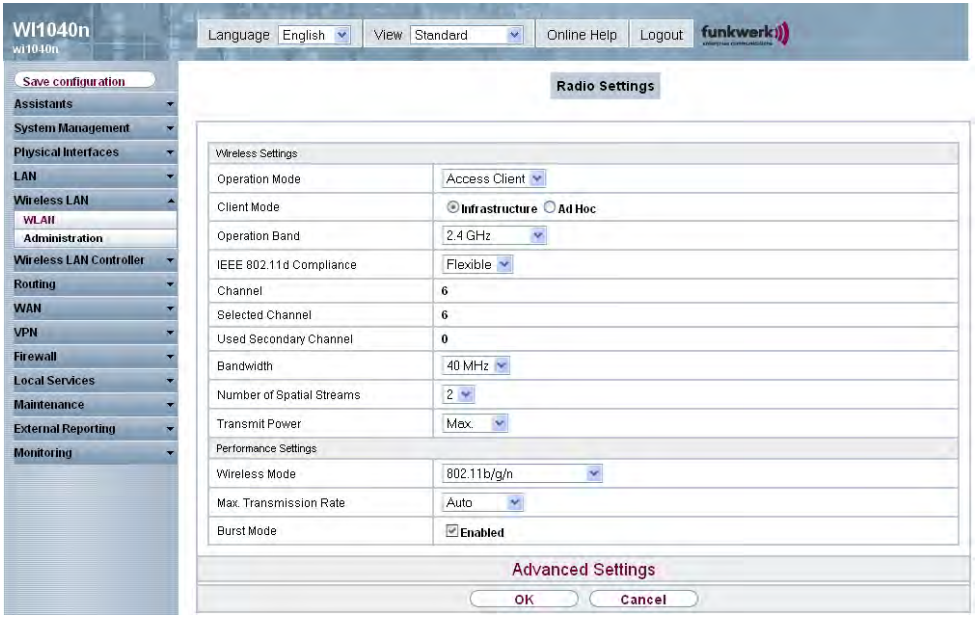


Fig. 62: **Wireless LAN WLAN Radio Settings** *for* **Operation Mode** = `Access Client`

The **Wireless LAN** -> **WLAN** -> **Radio Settings Settings** -> menu consists of the following fields:

Fields in the Radio Settings Wireless Settings menu

Field	Description
Operation Mode	Define the mode in which the wireless module of your device is to operate. Possible values: • `Off` (default value) The wireless module is not active. • `Access Point`: Your device is used as an access point in your network. • `Access Client`: Your device serves as an Access Client in your network. • `Bridge`: Your device is used as a wireless bridge in your network.
Client Mode	Only for **Operating Mode** = `Access Client` Possible values: • `Infrastructure` (default value): In a network in infrastruc-

Field	Description
	ture mode, all clients communicate with each other via access points only. There is no direct communication between the individual clients. • *Ad-Hoc*: In ad-hoc mode, an access client can be used as central interface between a number of terminals. In this way, devices such as computers and printers can be wirelessly interconnected. Select the **channel** to be used.
Operation Band	Select the operation band and usage area of the wireless module. For **Operation Mode** = *Access Point* or *Bridge* Possible values: • *2.4 GHz In/Outdoor* (default value): our device is operated at 2.4 GHz (mode 802.11b and mode 802.11g), inside or outside buildings. • *5 GHz Indoor*: Your device is run with 5 GHz (Mode 802.11a/h) inside buildings. • *5 GHz Outdoor*: Your device is run with 5 GHz (Mode 802.11a/h) outside buildings. • *5 GHz In/Outdoor*: Your device is run with 5 GHz (Mode 802.11a/h) inside or outside buildings. • 5.8 GHz Outdoor: Only for so-called Broadband Fixed Wireless Access (BFWA) applications. The frequencies in the frequency range from 5,755 MHz to 5,875 MHz may only be used in conjunction with commercial offers for public network accesses and requires registration with the Federal Network Agency. For **Operation Mode** = *Access Client* Possible values: • *2.4 and 5 GHz*(default value) • *5 GHz* • *2.4 GHz*
Usage Area	Only for **Operation Mode** = *Access Client*, **Client Mode** =

Field	Description
	Infrastructure and **Operation Band** = *2.4 and 5 GHz*or *5 GHz* Possible values: • *Indoor-Outdoor* (default value) • *Indoor* • *Outdoor*
IEEE 802.11d Compliance	Only for **Operating Mode** = *Access Client* Possible values: • *Flexible* (default value) • *None* • *Strict*
Channel	The number of channels you can selected depends on the country setting. Please consult the data sheet for your device. **Access Point Modus / Bridge Modus:** Configuring the network name (SSID) in Access Point mode means that wireless networks can be logically separated from each other, but they can still physically interfere with each other if they are operating on the same or closely adjacent wireless channels. So if you are operating two or more radio networks close to each other, it is advisable to allocate the networks to different channels. Each of these should be spaced at least four channels apart, as a network also partially occupies the adjacent channels. In the case of manual channel selection, please make sure first that the clients actually support these channels. Possible values: • For **Frequency Band** = *2.4 GHz In/Outdoor* Possible values are *1* to *13* and *Auto* (default value). *Auto* is not possible in bridge mode. • For **Frequency Band** = *5 GHz Indoor* Possible values are *36*, *40*, *44*, *48* and *Auto* (default value)

Field	Description
	• For **Operation Band** = *5 GHz In/Outdoor* and *5 GHz Outdoor* and *5.8 GHz Outdoor* Only the *Auto* option is possible here. **Access Client mode:** In Access Client mode you can only select the required channel in **Client Mode** = *Ad Hoc*. Possible values: • For **Frequency Band** = *2.4 GHz In/Outdoor* Possible values are *1* to *13* and *Auto* (default value). • For **Frequency Band** = *5 GHz Indoor* Possible values are *36*, *40*, *44*, *48* and *Auto* (default value) • For **Operation Band** = *5 GHz In/Outdoor* and *5 GHz Outdoor* and *5.8 GHz Outdoor* Only the *Auto* option is possible here.
Selected Channel	Displays the channel used.
Used Secondary Channel	Only for **Operation Mode** = *Access Client* or *Bridge* Displays the second channel used.
Bandwidth	Only for **Wireless Mode** = *802.11b/g/n*, *802.11g/n*, *802.11n*, *802.11a/n* Select how many channels are to be used. Possible values: • *20 MHz* (default value): One channel with 20 MHz bandwidth is used. • *40 MHz*: Two channels each with 20 MHz bandwidth are used. In the case one channel acts as a control channels and the other as an expansion channel.
Number of Spatial Streams	Only for **Wireless Mode** = *802.11b/g/n*, *802.11g/n*, *802.11n*, *802.11a/n*Select how many traffic flows are to be used in parallel.

Field	Description
	Possible values: • *2* (default value): Two traffic flows are used. • *1*: One traffic flow is used.
Max. Link Distance	Only for **Operation Mode** = *Bridge* Enter the maximum link range. If the *Use default* option is enabled, the automatically generated range is used. If this option is not enabled, enter the desired maximum value in the m field. The *Use default* option is enabled by default.
Transmit Power	Select the maximum value for the radiated antenna power. The actually radiated antenna power may be lower than the maximum value set, depending on the data rate transmitted. The maximum value for Transmit Power is country-dependent. Possible values: • *Max.* (default value): The maximum antenna power is used. • *5 dBm* • *8 dBm* • *11 dBm* • *14 dBm* • *16 dBm*

Fields in the Radio Settings Performance Settings menu

Field	Description
Wireless Mode	Select the wireless technology that the access point is to use. Only for **Operation Band** = *2.4 GHz In/Outdoor* Possible values: • *802.11g*: The device operates only in accordance with 802.11g. 802.11b clients have no access.

Field	Description
	• *802.11b*: Your device operates only in accordance with 802.11b and forces all clients to adapt to it. • *802.11 mixed (b/g)*: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. • *802.11 mixed-long (b/g)*: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. Only a data rate of 1 and 2 mbps needs to be supported by all clients (basic rates). This mode is also needed for Centrino clients if connection problems occur. • *802.11 mixed-short (b/g)*: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. The following applies for mixed-short: The data rates 5.5 and 11 mbps must be supported by all clients (basic rates). • *802.11 b/g/n*: Your device operates according to either 802.11b, 802.11g or 802.11n. • *802.11 g/n*: Your device operates according to either 802.11g or 802.11n. • *802.11 n*: Your device operates only according to 802.11n. In **Operation Mode** *Access Client* with **Client Mode** *Ad-Hoc* additional options are available for **Operation Band** = *5 GHz Indoor*, *5 GHz Outdoor*, *5 GHz In/Outdoor*, *5.8 GHz Outdoor*. Possible values: • *802.11a*: The device operates only in accordance with 802.11a. • *802.11n*: Your device operates only according to 802.11n. • *802.11 a/n*: Your device operates according to either 802.11a or 802.11n. • *802.11a/b/g/n* (read only): Only in **Operation Mode** *Access Client* with **Client Mode** *Infrastructure*.
Max. Transmission Rate	Select the transmission speed. Possible values: • *Auto* (default value): The transmission speed is determined

Field	Description
	automatically. • *<Value>*: Depending on the setting for **Operation Band**, **Bandwidth**, **Number of spatial streams** and **Wireless Mode**, different whole values in mbps will be available for selection.
Burst Mode	Activate this function to increase the transmission speed for 802.11g through frame bursting. As a result, several packets are sent one after the other without a waiting period. This is particularly effective in 11b/g mixed operation. The function is activated with *Enabled*. The function is activated by default. If problems occur with older WLAN hardware, this function should be deactivated.

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Channel Plan	Only for **Operation Mode** = *Access Point* and **Channel** = *Auto*. Select the desired channel plan. The channel plan makes a preselection when a channel is selected. This ensures that no channels overlap, i.e. a distance of four channels is maintained between the channels used. This is useful if more access points are used with overlapping radio cells. Possible values: • *All*: All channels can be dialled when a channel is selected. • *Auto*: Depending on the region, operation band, wireless mode and bandwidth, the channels that have a distance of 4 channels are provided. • *User Defined*: Select the desired channels.
Beacon Period	Only if **Operation Mode** = *Access Point* or *Access Client* with **Client Mode** *Ad Hoc*.

Field	Description
	Enter the time in milliseconds between the sending of two beacons. This value is transmitted in Beacon and Probe Response Frames. Possible values are *1* to *65535*. The default value is *100* msec.
DTIM Period	Only if **Operation Mode** = *Access Point* or *Access Client* with **Client Mode** *Ad Hoc*. Enter the interval for the Delivery Traffic Indication Message (DTIM). The DTIM field is a data field in transmitted beacons that informs clients about the window to the next broadcast or multicast transmission. If clients operate in power save mode, they come alive at the right time and receive the data. Possible values are *1* to *255*. The default value is *2*.
RTS Threshold	Here, you select how the RTS/CTS mechanism is to be switched on/off. If you choose *User Defined*, in the input field you can specify the data packet length threshold in bytes (1..2346) as of which the RTS/CTS mechanism is to be used. This makes sense if several clients that are not in each other's wireless range are run in one access point. The mechanism can also be switched on/off independently of the data packet length by selecting the value *Always on* or *Always off* (default value).
Short Guard Interval	Enable this function to reduce the guard interval (= time between transmission of two data symbols) from 800ns to 400ns.
Short Retry Limit	Enter the maximum number of attempts to send a frame of length less than or equal to the value defined in **RTS Threshold**. After this many failed attempts, the packet is discarded.

Field	Description
	Possible values are *1* to *255*. The default value is *7*.
Long Retry Limit	Enter the maximum number of attempts to send a data packet of length less than or equal to the value defined in **RTS Threshold**. After this many failed attempts, the packet is discarded. Possible values are *1* to *255*. The default value is *4*.
Fragmentation Threshold	Enter the maximum size as of which the data packets are to be fragmented (i.e. split into smaller units). A low value is recommended for this field in areas with poor reception and in the event of radio interference. Possible values are *256* to *2346*. The default value is *2346* bytes.

If *Access Client* has been selected for the **Operation Mode** with **Client Mode** *Infrastructure*, the following parameters will also be available under **Advanced Settings**.

Fig. 63: **Wireless LAN** -> **WLANx** -> **Wireless Module Settings**-> ->**Advanced Settings** *for* **Operation Mode** *Access Client*

Fields in the Advanced Settings Access Client Mode menu

Field	Description
Scan channels	Choose the channels which the WLAN client automatically scans for available wireless networks. Possible values: • *All* (default value): All channels are scanned. • *Auto*: The channel is automatically selected. • *User Defined*: The desired channels can therefore be defined.
Roaming Profile	Select the roaming profile. The options available include typical roaming functions. Possible values: • *Fast Roaming*: The WLAN client searches for available wireless networks as soon as the radio signal of the existing radio connection becomes unsuitable for higher data rates. • *Normal Roaming* (default value): Standard roaming. • *Slow Roaming*: The WLAN client searches for available wireless networks as soon as the radio signal of the existing radio connection becomes weaker. • *No Roaming*: The WLAN client searches for available wireless networks if it is no longer connected to a wireless network. • *Custom Roaming*: Specify the individual roaming parameters.
Scan Threshold	Indicates the value in dBm above which the system scans for available wireless networks in the background. The value can only be changed for **Roaming Profile** = *Custom Roaming*. The default value is *-70 dBm*.
Scan Interval	Indicates the interval in milliseconds after which the system scans for available wireless networks. The value can only be changed for **Roaming Profile** = *Custom Roaming*. The default value is *5000 ms*.
Channel Sweep	Indicates how many frequencies are scanned in the background. The value can only be changed for **Roaming Profile** = *Custom*

Field	Description
	Roaming. The default value is *2*. The value *0* disables the scan in the background. The value *-1* enables the scan of all available frequencies.
Min. Time Period for Active Scan	Indicates the minimum time in milliseconds a frequency is actively scanned. The value can only be changed for **Roaming Profile** = *Custom Roaming*. The default value is *10 ms*.
Max. Time Period for Active Scan	Indicates the maximum time in milliseconds a frequency is actively scanned. The value can only be changed for **Roaming Profile** = *Custom Roaming*. The default value is *40 ms*.
Min. Time Period for Passive Scan	Indicates the minimum time in milliseconds a frequency is passively scanned. The value can only be changed for **Roaming Profile** = *Custom Roaming*. The default value is *20 ms*.
Max. Time Period for Passive Scan	Indicates the maximum time in milliseconds a frequency is actively scanned. The value can only be changed for **Roaming Profile** = *Custom Roaming*. The default value is *120 ms*.
RTS Threshold	Select how the RTS/CTS mechanism is to be switched on/off. If you choose *User Defined*, in the input field you can specify the data packet length threshold in bytes (1..2346) as of which the RTS/CTS mechanism is to be used. This makes sense if several clients that are not in each other's wireless range are run in one access point. The mechanism can also be switched on/off independently of the data packet length by selecting the value *Always on* or *Always off* (default value).
Short Guard Interval	Enable this function to reduce the guard interval (= time between transmission of two data symbols) from 800ns to 400ns.
Short Retry Limit	Enter the maximum number of attempts to send a frame of length less than or equal to the value defined in **RTS Threshold**. After this many failed attempts, the packet is discarded.

Field	Description
	Possible values are *1* to *255*. The default value is *7*.
Long Retry Limit	Enter the maximum number of attempts to send a data packet of length less than or equal to the value defined in **RTS Threshold**. After this many failed attempts, the packet is discarded. Possible values are *1* to *255*. The default value is *4*.
Fragmentation Threshold	Enter the maximum size as of which the data packets are to be fragmented (i.e. split into smaller units). A low value is recommended for this field in areas with poor reception and in the event of radio interference. Possible values are *256* to *2346*. The default value is *2346* bytes.

12.1.2 Virtual Service Sets

If you operate your device in access point mode (**Wireless LAN** -> **WLAN** -> **Radio Settings** ->->**Operation Mode** = *Access Point*), you can set up and edit the desired wireless networks in the **Wireless LAN** -> **WLAN** -> **Wireless Networks (VSS)**->->**/New** menu.

Note

The preset wireless network Funkwerk-EC has the following security settings in the ex works state:

- **Security Mode** = *WPA-PSK*
- **WPA Mode** = *WPA and WPA2*
- **WPA Cipher** and **WPA2 Cipher** = *AES and TKIP*
- The **Preshared Key** is filled with an internal system value, which you must change during configuration.

Setting network names

In contrast to a LAN set up over Ethernet, a wireless LAN does not have any cables for setting up a permanent connection between the server and clients. Access violations or faults may therefore occur with directly adjacent radio networks. To prevent this, every radio network has a parameter that uniquely identifies the network and is comparable with a domain name. Only clients with a network configuration that matches that of your device can communicate in this WLAN. The corresponding parameter is called the network name. In the network environment, it is sometimes also referred to as the SSID.

Protection of wireless networks

As data can be transmitted over the air in the WLAN, this data can in theory be intercepted and read by any attacker with the appropriate resources. Particular attention must therefore be paid to protecting the wireless connection.

There are three security modes, WEP, WPA-PSK and WPA Enterprise. WPA Enterprise offers the highest level of security, but this security mode is only really suitable for companies, because it requires a central authentication server. Private users should choose WEP or preferably WPA-PSK with higher security as their security mode.

WEP

802.11 defines the WEP security standard (Wired Equivalent Privacy = encryption of data with 40 bits (**Security Mode** = *WEP 40*) or 104 bits (**Security Mode** = *WEP 104*). However, this widely used WEP has proven susceptible to failure. However, a higher degree of security can only be achieved through hardware-based encryption which required additional configuration (for example 3DES or AES). This permits even sensitive data from being transferred via a radio path without fear of it being stolen.

IEEE 802.11i

Standard IEEE 802.11i for wireless systems contains basic security specifications for wireless networks, in particular with regard to encryption. It replaces the insecure WEP (Wired Equivalent Privacy) with WPA (Wi-Fi Protected Access). It also includes the use of the advanced encryption standard (AES) to encrypt data.

WPA

WPA (Wi-Fi Protected Access) offers additional privacy by means of dynamic keys based on the Temporal Key Integrity Protocol (TKIP), and offers PSK (preshared keys) or Extensible Authentication Protocol (EAP) via 802.1x (e.g. RADIUS) for user authentication.

Authentication using EAP is usually used in large wireless LAN installations, as an authentication instance in the form of a server (e.g. a RADIUS server) is used in these cases. PSK (preshared keys) are usually used in smaller networks, such as those seen in SoHo (Small

office, Home office). Therefore, all the wireless LAN subscribers must know the PSK, because it is used to generate the session key.

WPA2

WPA2 is the enhancement of WPA. In WPA2, the 802.11i standard is not only implemented for the first time in full, but another encryption algorithm AES (Advanced Encryption Standard) is also used.

Access control

You can control which clients can access your wireless LAN via your device by creating an Access control list (**ACL Mode** or **MAC Filter**). In the Access Control List, you enter the MAC addresses of the clients that may access your wireless LAN. All other clients have no access.

Security measures

To protect the data transferred on the WLAN, you may need to carry out the following configuration steps in the **Wireless LAN** -> **WLAN** -> **Wireless Networks (VSS)**->**New**->/ menu:

- Change the access passwords for your device.
- Change the default SSID, **Network Name (SSID)** = *Funkwerk-ec* , of your access point. Set **Visible** = *Enabled*. This will exclude all WLAN clients that attempt to establish a connection with the general value for **Network Name (SSID)** *Any* and do not know the SSID settings.
- Use the available encryption methods. To do this, select **Security Mode** = *WEP 40*, *WEP 104* , *WPA PSK* or *WPA Enterprise* or both, and enter the relevant key in the access point under **WEP Key1 - 4** or **Preshared Key** and in the WLAN clients.
- The WEP key should be changed regularly. To do this, change the **Transmit Key**. Select the longer 104 Bit WEP key.
- For the transfer of highly security-critical informationen, **Security Mode** = *WPA-Enterprise* should be configured with **WPA Mode** = *WPA 2*. This method contains hardware-based encryption and RADIUS authentication of the client. In special cases, combination with IPSec is possible.
- Restrict WLAN access to permitted clients. Enter the MAC addresses of the wireless network cards of these clients in the **Allowed Addresses**-list in the **MAC Filter** menu (see *Fields in the MAC Filter menu* on page 161).

In the **Wireless LAN** -> **WLAN** -> **Virtual Service Sets** menu, a list of all WLAN networks shown.

12.1.2.1 Virtual Service Sets ->New/

Choose the icon to edit existing entries. Choose the **New** button to configure other wireless networks.

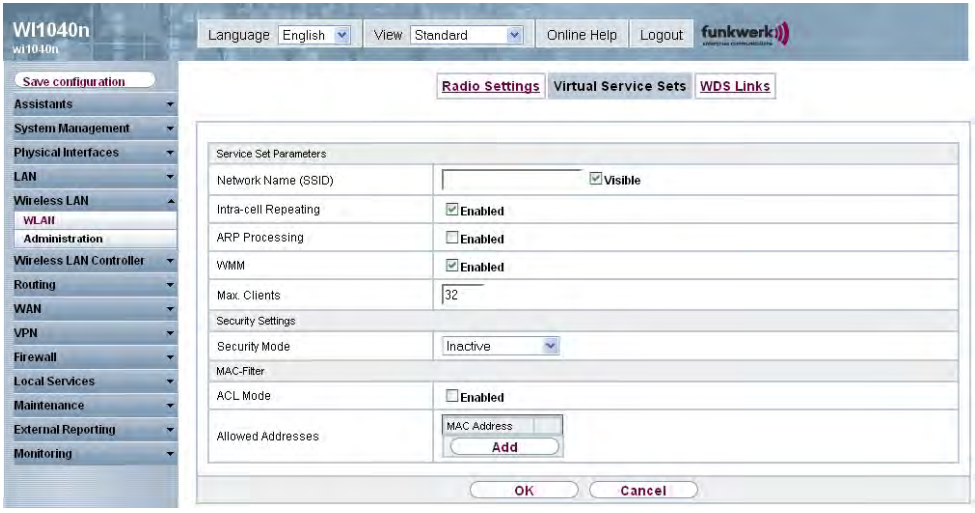


Fig. 64: **Wireless LAN -> WLAN -> Wireless Networks (VSS)->->/New**

The **Wireless LAN -> WLAN -> Wireless Networks (VSS)->->/New** menu consists of the following fields:

Fields in the Virtual Service Sets Service Set Parameters menu

Field	Description
Network Name (SSID)	Enter the name of the wireless network (SSID). Enter an ASCII string with a maximum of 32 characters. Also select whether the **Network Name (SSID)** is to be transmitted. The network name is shown by choosing *Visible*. It is visible by default.
Intra-cell Repeating	Select whether communication between the WLAN clients is to be permitted within a radio cell. The function is activated by choosing *Enabled*.

Field	Description
	The function is enabled by default.
ARP Processing	Select whether the ARP processing function should be enabled. The ARP data traffic is reduced in the network by the fact that ARP broadcasts that have been converted to ARP unicasts are forwarded to IP addresses that are known internally. Unicasts are quicker and clients with an enabled power save function are not addressed. The function is activated by choosing *Enabled*. The function is disabled by default. Make sure that ARP processing cannot be applied in conjunction with the MAC bridge function.
WMM	Select whether voice or video prioritisation via WMM (Wireless Multimedia) is to be activated for the wireless network so that optimum transmission quality is always achieved for time-critical applications. Data prioritisation is supported in accordance with DSCP (Differentiated Services Code Point) or IEEE802.1d. The function is activated by choosing *Enabled*. The function is enabled by default.
Max. Clients	Enter the maximum number of clients that can be connected to this wireless network (SSID) The maximum number of clients that can register with a wireless module depends on the specifications of the respective WLAN module. This number can be shared across all configured wireless networks. If the maximum number of clients is reached, no more new wireless networks can be created and a warning message will appear.

Fields in the Virtual Service Sets Security Settings menu

Field	Description
Security Mode	Select the security mode (encryption and authentication) for the wireless network. Possible values:

Field	Description
	• *Inactive* (default value): Neither encryption nor authentication • *WEP 40*: WEP 40 Bit • *WEP 104*: WEP 104 Bit • *WPA-PSK*: WPA Preshared Key • *WPA-Enterprise*: 802.11x
Transmit Key	Only if **Security Mode** = *WEP 40, WEP 104* Select one of the keys configured in **WEP Key <1 - 4>** as the default key. The default value is *Key 1*.
WEP Key 1-4	Only if **Security Mode** = *WEP 40* , *WEP 104* Enter the WEP key. Enter a character string with the right number of characters for the selected WEP mode. For *WEP 40* you need a string of 5 characters, *WEP 104* 13 characters. For example *hello* for *WEP 40*, *funkwerk-wep1* for *WEP 104*.
WPA Mode	Only if **Security Mode** = *WPA-PSK* and *WPA-Enterprise* Select whether you want to use WPA (with TKIP encryption) or WPA 2 (with AES encryption), or both. Possible values: • *WPA and WPA 2* (default value): WPA and WPA 2 can be used. • *WPA* : Only WPA is used. • *WPA 2* : Only WPA2 is used.
WPA Cipher	Only for **Security Mode** = *WPA-PSK* and *WPA-Enterprise* and for **WPA Mode** = *WPA* and *WPA and WPA2* Select the type of encryption you want to apply to WPA. Possible values: • *Please select a valid option.* (default value)

Field	Description
	• *AES*: AES is used. • *AES and TKIP*: AES or TKIP is used.
WPA2 Cipher	Only for **Security Mode** = *WPA-PSK* and *WPA-Enterprise* and for **WPA Mode** = *WPA2* and *WPA and WPA2* Select the type of encryption you want to apply to WPA2. Possible values: • *AES* (default value): AES is used. • *AES and TKIP*: AES or TKIP is used.
Preshared Key	Only if **Security Mode** = *WPA-PSK* Enter the WPA password. Enter an ASCII string with 8 - 63 characters. Note: Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorised access!
EAP Preauthentification	Only if **Security Mode** = *WPA-Enterprise* Select whether the EAP preauthentification function is to be activated. This function tells your device that WLAN clients, which are already connected to another access point, can first carry out 802.1x authentication as soon as they are within range. Such WLAN clients can then simply connect over the existing network connection with your device. The function is activated by choosing *Enabled*. The function is enabled by default.

Fields in the MAC Filter menu

Field	Description
ACL Mode	Select whether only certain clients are to be permitted for this wireless network. The function is activated by choosing *Enabled*. The function is disabled by default.

Field	Description
Allowed Addresses	Use **Add** to make entries and enter the MAC addresses (**MAC Address**) of the clients to be permitted.

12.1.3 WDS Links

If you operate your device in access point mode (**Wireless LAN** -> **WLAN** -> **Wireless Module Settings**-> ->**Operation Mode** = *Access Point*), you can set up and edit the desired WDS links in the **Wireless LAN** -> **WLAN** -> **WDS Links**-> ->**/New** menu.

Important

The WDS link can only be configured in the 2.4 GHz band and in the 5 GHz band indoor if the channel is NOT *Auto*.

The number of channels you can selected depends on the country setting. Please consult the data sheet for your device.

WDS links (WDS = Wireless Distribution System) are static links between access points (AP), which are generally used to connect clients with networks that are not directly accessible to them e.g. because the distance is too great. The access point sends from one client to another access point, which then forwards the data to another client.

Important

Note that the data is transferred between the access points in unencrypted form over the WDS link in the default configuration. You are therefore urgently advised to apply one of the available security methods (WEP40 or WEP104) to protect data on WDS links.

WDS links are configured as interfaces with the prefix *wds*. They behave like VSS interface and only differ from these with respect to the predefined routing. A WDS link is defined as a transit network: this relates to a point-to-point connection or point-to-multipoint connection between two access points that are included in different networks.

12.1.3.1 WDS Links -> New/

Choose the icon to edit existing entries. Choose the **New** button to configure other WDS links.

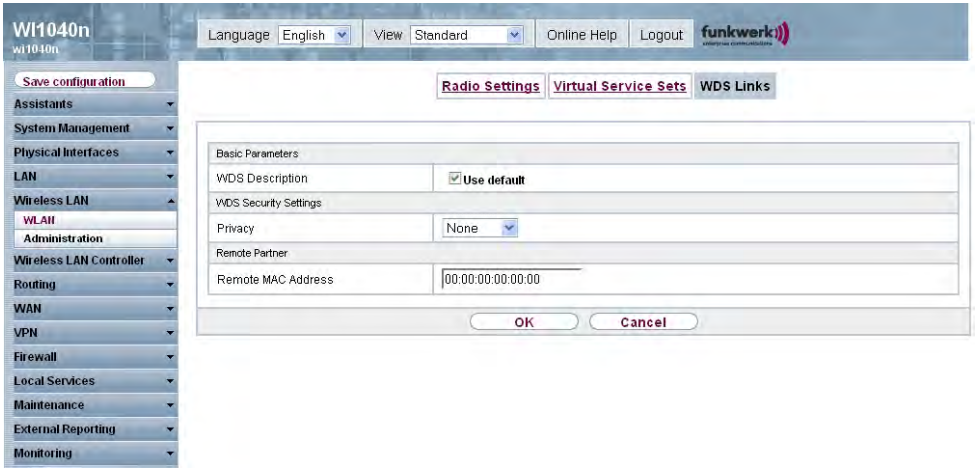


Fig. 65: **Wireless LAN -> WLAN -> WDS Links->->/New**

The **Wireless LAN -> WLAN -> WDS Links->->/New** menu consists of the following fields:

Fields in the WDS Links Basic Parameters menu

Field	Description
WDS Description	Enter a name for the WDS link. If the *Use Standard* option is activated, the generated name of the interface is automatically used. If the option is not activated, you can enter a suitable name in the input field. The *Use Standard* option is enabled by default.

Fields in the WDS Security Settings menu

Field	Description
Privacy	Select whether an encryption method is to be used for this WDS link and if so, which one. Possible values: • *None* (default value): Data traffic on this WDS link is not encrypted. • *WEP40*: Data traffic on this WDS link is encrypted with WEP40. In **WEP Key 1 - 4**, enter the key for this WDS link

Field	Description
	and in **Transmission Key**, select the default key. • *WEP104*: Data traffic on this WDS link is encrypted with WEP104. In **WEP Key 1 - 4**, enter the key for this WDS link and in **Transmission Key**, select the default key. • *WPA* : Data traffic on this WDS link is encrypted with WPA. Enter the key for this WDS link in **Preshared Key**. • *WPA 2* : Data traffic on this WDS link is encrypted with WPA. Enter the key for this WDS link in **Preshared Key**.
Transmit Key	Only if **Privacy** = *WEP40* , *WEP104* Select one of the keys configured in **WEP Key <1 - 4>** as the default key. The default value is *Key 1*.
WEP Key 1 - 4	Only if **Privacy** = *WEP40*, *WEP104* Enter the WEP key. There are two ways of entering a WEP key: • Direct entry in hexadecimal form If the entry starts with *0x*, the generator is deactivated. Enter a hexadecimal string with exactly the right number of characters for the selected WEP mode. 10 characters for *WEP40* or 26 characters for *WEP104* e.g. *WEP40*: *0xA0B23574C5*, *WEP104*: *0x81DC9BDB52D04DC20036DBD831* • Direct entry of ASCII characters Enter a character string with the right number of characters for the selected WEP mode. For *WEP40* you need a string of 5 characters, *WEP104* 13 characters. For example *hello* for *WEP40*, *funkwerk-wep1* for *WEP104*.
Preshared Key	Only if **Privacy** = *WPA* , *WPA 2* Enter the WPA password. Enter an ASCII string with 8 - 63 characters.

Fields in the Remote Partner menu

Field	Description
Remote MAC Address	Enter the MAC address of the WDS partner.

12.1.4 Client Link

If you operate your device in access client mode (**Wireless LAN** -> **WLAN** -> **Radio Settings**->->**Operation Mode** = `Access Client`), you can edit the available Client Links in the **Wireless LAN** -> **WLANx** -> **Client Links**->-> menu.

The client mode can be operated in infrastructure mode or in ad-hoc mode.

In a network in infrastructure mode, all clients communicate with each other via access points only. There is no direct communication between the individual clients.

In ad-hoc mode, an access client can be used as central interface between a number of terminals. In this way, devices such as computers and printers can be wirelessly interconnected.

12.1.4.1 Client Link ->

Choose the icon to edit existing entries.

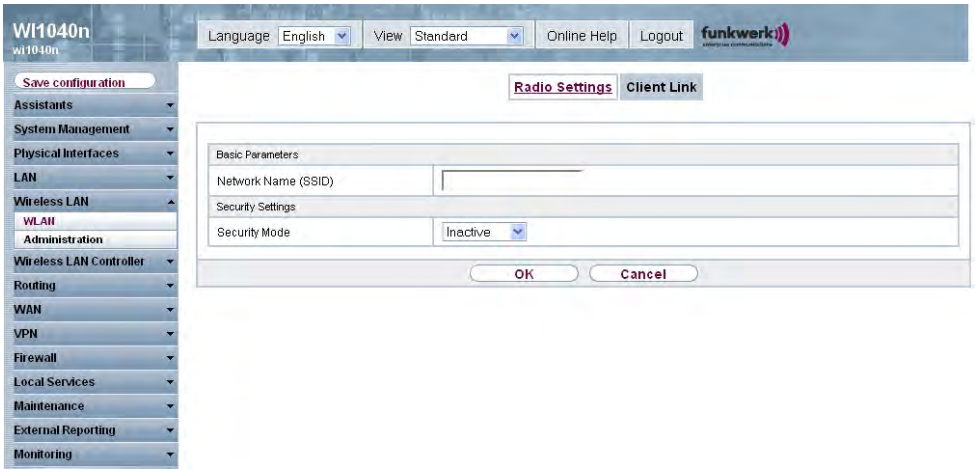


Fig. 66: **Wireless LAN** -> **WLAN** -> **Client Link**->->

The **Wireless LAN** -> **WLAN** -> **Client Link**->-> menu consists of the following fields:

Fields in the Client Link Basic Parameters menu

Field	Description
Network Name (SSID)	Enter the name of the wireless network (SSID). Enter an ASCII string with a maximum of 32 characters.

Fields in the Client Link Security Settings menu

Field	Description
Security Mode	Select the security mode (encryption and authentication) for the wireless network. Possible values: • *Inactive* (default value): Neither encryption nor authentication • *WEP 40*: WEP 40 Bit • *WEP 104*: WEP 104 Bit • *WPA None*: Only if **Client Mode** = *Ad Hoc*. WPA None: • *WPA-PSK*: Only if **Client Mode** = *Infrastructure*. WPA Preshared Key
Transmit Key	Only if **Security Mode** = *WEP 40, WEP 104* Select one of the keys configured in **WEP Key <1 - 4>** as the default key. The default value is *Key 1*.
WEP Key 1-4	Only if **Security Mode** = *WEP 40* , *WEP 104* Enter the WEP key. Enter a character string with the right number of characters for the selected WEP mode. For *WEP 40* you need a string of 5 characters, *WEP 104* 13 characters. For example *hello* for *WEP 40*, *funkwerk-wep1* for *WEP 104*.
WPA Mode	Only if **Security Mode** = *WPA-PSK* Select whether you want to use WPA (with TKIP encryption) or WPA 2 (with AES encryption), or both. Possible values:

Field	Description
	• *WPA* (default value): Only WPA is used. • *WPA 2* : Only WPA2 is used.
Preshared Key	Only if **Security Mode** = *WPA-PSK* Enter the WPA password. Enter an ASCII string with 8 - 63 characters.
WPA Cipher	Only for **Security Mode** = *WPA-PSK* and **WPA Mode** = *WPA* Select which encryption method should be used. Possible values: • *TKIP* (default value): Temporal Key Integrity Protocol. • *AES*: Advanced Encryption Standard. • *AES and TKIP* Both encryption methods are rated as secure, with AES offering better performance.
WPA2 Cipher	Only for **Security Mode** = *WPA-PSK* and **WPA Mode** = *WPA2* Select which encryption method should be used. Possible values: • *TKIP* (default value): Temporal Key Integrity Protocol. • *AES*: Advanced Encryption Standard. • *AES and TKIP* Both encryption methods are rated as secure, with AES offering better performance.

12.1.4.2 Client Link Scan

After the desired **Client Links** have been configured, the icon is shown in the list.

You use this icon to open the **Scan** menu.

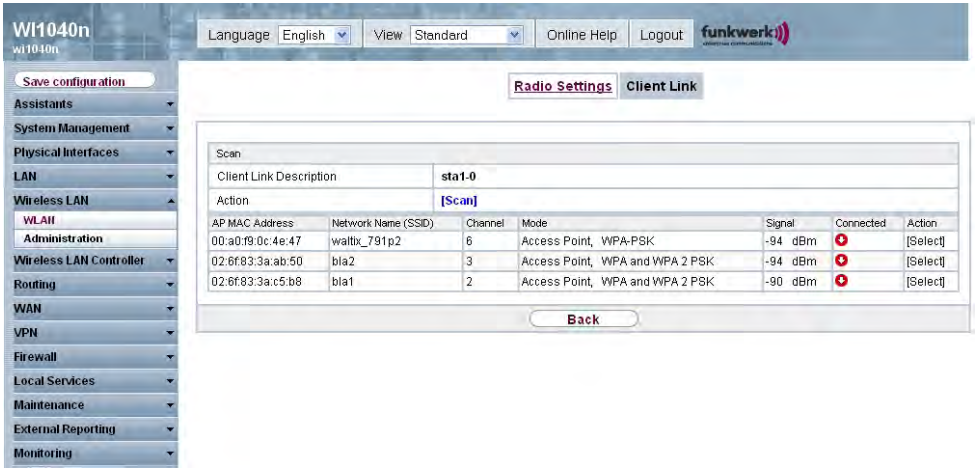


Fig. 67: **Wireless LAN** -> **WLAN** -> **Client Link**->**Scan**

After successful scanning, a selection of potential scan partners is displayed in the scan list. In the **Action** column, click **[Select]** to connect the local clients with this client. If the partners are connected with one another, the icon appears in the **Connected** column. The icon appears in the **Connected** column if the connection is active.

The **Wireless LAN** -> **WLAN** -> **Client Link** -> **Scan** menu consists of the following fields:

Fields in the Client Link Scan menu

Field	Description
Client Link Description	Displays the name of the client link you configured.
Action	Start the scan by clicking on **Scan**. If the antennas are installed correctly on both sides and LOS is free, the client finds available clients and displays them in the following list. If the partner client cannot be found, check the line of sight and the antenna installation. Then carry out the **Scan** again. The partner should then be found.
AP MAC Address	Shows the MAC address of the remote client.
Network Name (SSID)	Displays the name of the remote client.
Channel	Shows the **Channel** used.
Mode	Shows the security mode (encryption and authentication) for the wireless network.

Field	Description
Signal	Displays the signal strength of the detected client link in dBm.
Connected	Displays the status of the link on your client.
Action	You can change the status of the client link. The available actions are displayed in this field.

12.1.5 Bridge Links

If you operate your device in bridge mode (**Wireless LAN** -> **WLAN** -> **Radio Settings**-> ->**Operation Mode** = *Bridge*), you can set up and edit the desired bridge links in the **Wireless LAN** -> **WLAN** -> **Bridge Links**-> ->**/New** menu.

With the bridge function, you can, for example, make a wireless connection between a **bintec W1002n** and one or more other **bintec W1002n** devices. The range of these wireless connections can be several kilometres, depending on the antennas used.

Note

Always use the antennas and antenna cables supplied with the equipment to prevent unintentional violations of the applicable law. If you have special requirements, e.g. regarding cable lengths, please contact your dealer or Funkwerk Enterprise Communications GmbH.

Bridges are generally used to interconnect various LAN segments at Layer 2 of the OSI 7-layer model. The special feature of **bintec** bridges is that the distances between these segments can be several kilometres, without the necessity for a cable for these ranges.

If you operate a wireless port in Bridge mode, this can only be used for a bridge link. This means:

- The port has no network name.
- Wireless clients cannot log in (associate) to this port.
- There is no node table for this port (as there are no clients).
- There is no Access Control List (ACL) for this port.

This port will only connect to the partner bridge port you have configured and also only accept connections from this port.

The **bintec** bridges have transmission rates far above the possibilities of the ISDN S0, ISDN S2M or ADSL. The high-speed bridge bridge even surpasses standard Ethernet (10BaseT, 10Base2, 10Base5).

Caution

Never connect two bridges that have set up a connection to each other with radio to the same LAN segment. This leads to unavoidable overloading of your network and stops all network traffic.

Some of the possible network topologies are described here to give you an overview of the options available when you use **bintec** bridges.

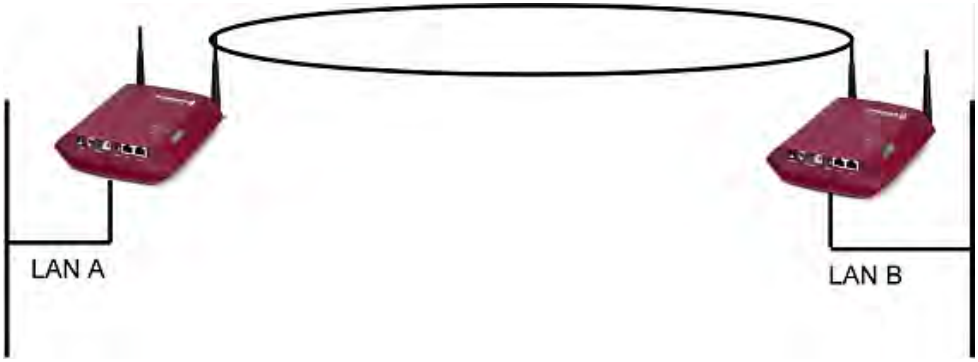


Fig. 68: Point-to-point topology

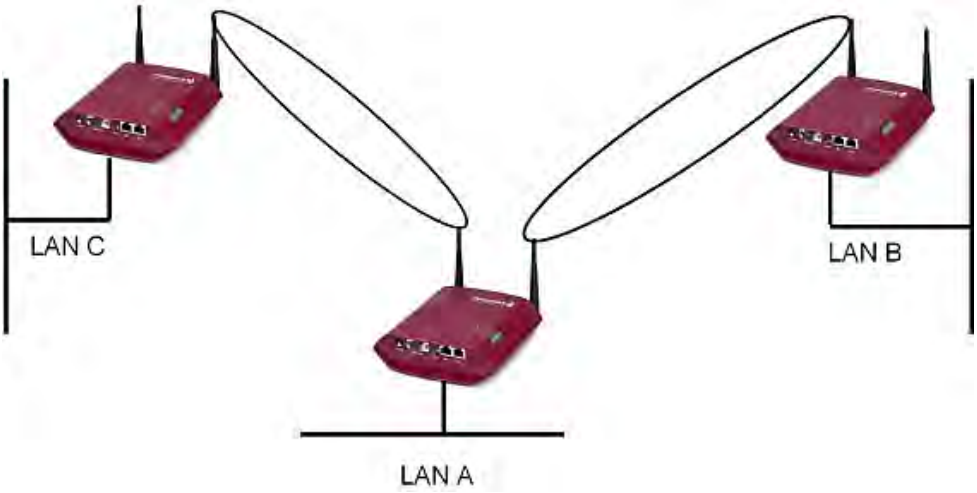


Fig. 69: Point-to-multipoint topology

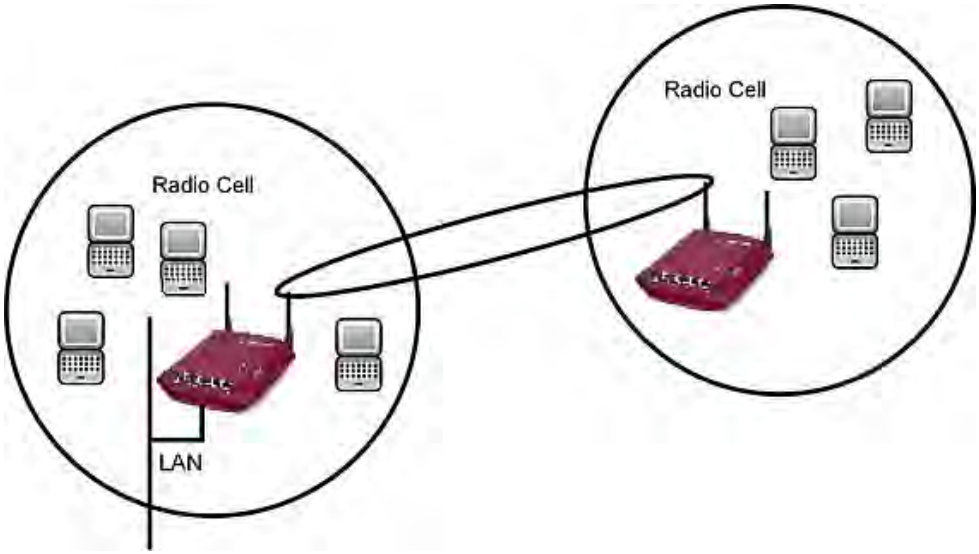


Fig. 70: Wireless backbone

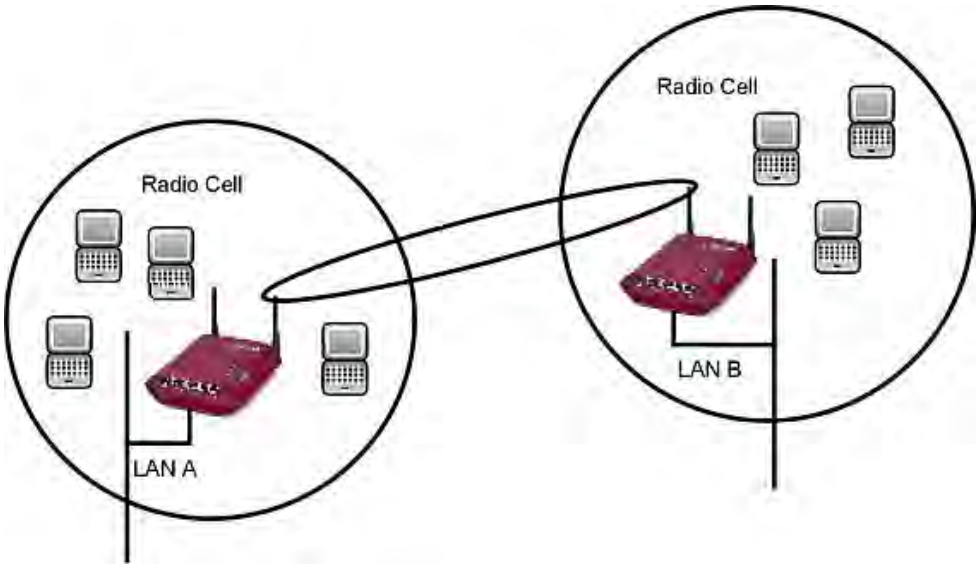


Fig. 71: Wireless bridge with connection of wireless clients

To be able to set up a wireless link to **bintec** bridges, an uninterrupted view must exist between the antennas at both ends. This is called a line of sight, abbreviated to LOS.

The term line of sight does not just mean a straight line of vision between the two antennas, but a kind of tunnel, which must not be disturbed by obstacles. This tunnel is called the 1st Fresnel zone. The Fresnel zone has the shape of an ellipse rotated around its lon-

gitudinal axis. At least 60 % of the 1st Fresnel zone must remain free of obstacles. The radius (or the small semi-axis) depends on the frequency used and the distance between the antennas.

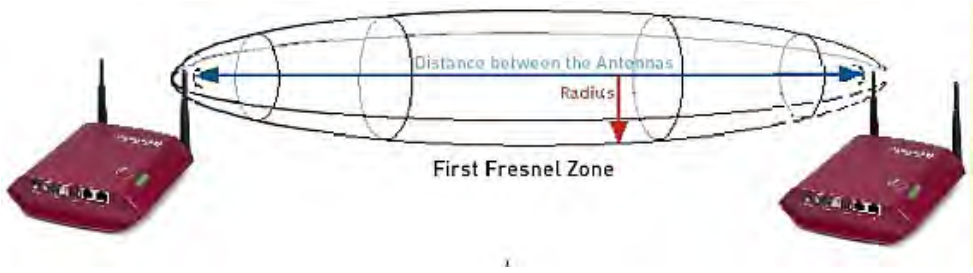


Fig. 72: 1. Fresnel zone

Example: Radius of 1st Fresnel zone as a function of distance from transmit antenna for antenna separation of 5 km at 2.45 GHz.

Example 1

Distance from transmit antenna (km)	Radius of 1st Fresnel zone (m)	Radius at 60 % of 1st Fresnel zone (m)
0,250	5,4	4,2
0,500	7,4	5,7
0,750	8,8	6,8
1,000	9,9	7,7
1,250	10,7	8,3
1,500	11,3	8,8
1,750	11,8	9,1
2,000	12,1	9,4
2,250	12,3	9,5
2,500	12,4	9,6
2,750	12,3	9,5
3,000	12,1	9,4
3,250	11,8	9,1
3,500	11,3	8,8
3,750	10,7	8,3
4,000	9,9	7,7
4,250	8,8	6,8

Distance from transmit antenna (km)	Radius of 1st Fresnel zone (m)	Radius at 60 % of 1st Fresnel zone (m)
4,500	7,4	5,7
4,750	5,4	4,2

Example: Radius of 1st Fresnel zone as a function of distance to the transmit antenna for a distance of 700 m at 2.45 GHz.

Example 2

Distance from transmit antenna (km)	Radius of 1st Fresnel zone (m)	Radius at 60 % of 1st Fresnel zone (m)
100	1,6	1,25
200	2,1	1,6
300	2,3	1,75
400	2,3	1,75
500	2,	1,6
600	1,6	1,25

Note

When setting up a bridge link, make sure that no obstacles or trees protrude into the Fresnel zone. If obstacles exist, the transmission rate will drop and the path may eventually fail.

It is not essential to consider the LOS for short distances inside buildings, as the radius of the Fresnel zone will be very small here.

If you meet these requirements, the link can be set up and maintained without further limitations. A special feature of links with **bintec** bridges is that they are completely unaffected by weather conditions.

Note

For a bridge path, always use the marked antenna connection. This is the device's primary connection.

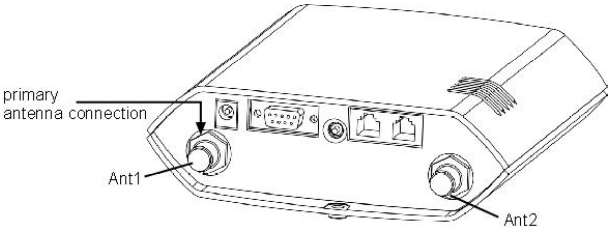


Fig. 73: Antenna connection

A label containing details of the two antennas is located on the back of the device. The primary antenna is designated **Ant 1**.

12.1.5.1 Bridge Links -> New/

Choose the icon to edit existing entries. Choose the **New** button to configure other bridge links.

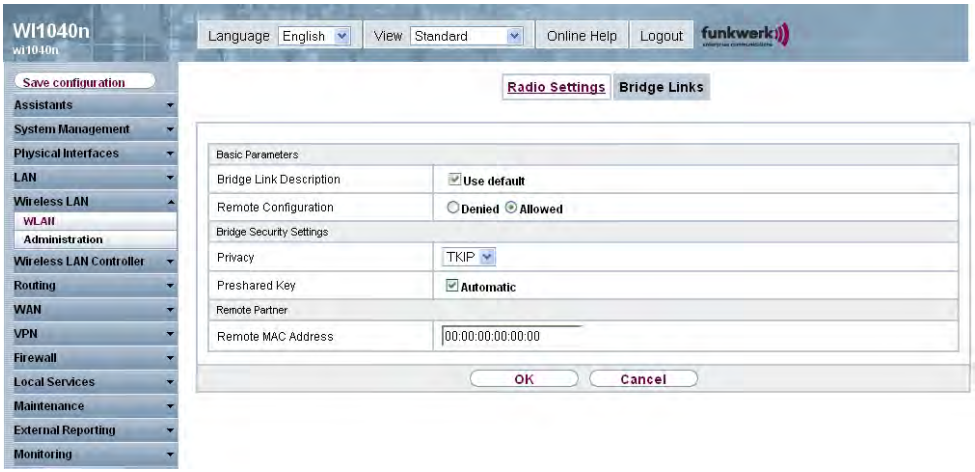


Fig. 74: **Wireless LAN -> WLAN -> Bridge Links-> ->/New**

The **Wireless LAN -> WLAN -> Bridge Links-> ->/New** menu consists of the following fields:

Fields in the Bridge Links Basic Parameters menu

Field	Description
Bridge Link Description	Enter a name for the bridge link. If the *Use Standard* option is activated, the generated name of the interface is automatically used.

Field	Description
	If the option is not activated, you can enter a suitable name in the input field. The *Use Standard* option is enabled by default.
Remote Configuration	Select whether setup of a bridge link from a remote bridge is to be permitted. Possible values: • *Allowed* (default value): It is possible to set up a bridge link from a remote bridge. • *Denied*: It is not possible to set up a bridge link from a remote bridge.

Fields in the Bridge Links Bridge Security Settings menu

Field	Description
Privacy	Select whether an encryption method is to be used for this bridge link and if so, which one. Possible values: • *TKIP* (default value): Temporal Key Integrity Protocol. • *AES*: Advanced Encryption Standard. Both encryption methods are rated as secure, with AES offering better performance.
Preshared Key	Enter the password for this bridge link. You can also obtain the preshared key automatically.

Fields in the Bridge Links Remote Partner menu

Field	Description
Remote MAC Address	Enter the MAC address of the bridge link partner.

12.1.5.2 Bridge Links Scan

After the desired **Bridge Links** have been configured, the icon is shown in the list.

You can use this icon to open the **Automatic Bridge Link Configuration** menu.

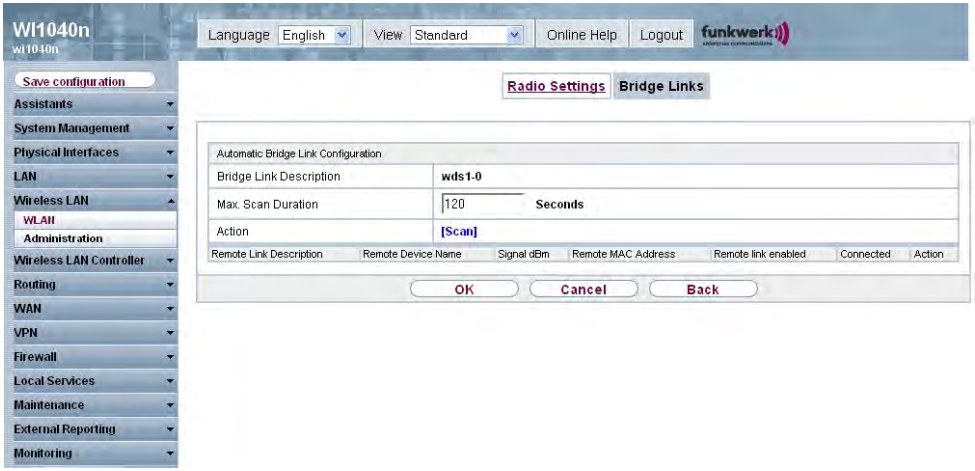


Fig. 75: **Wireless LAN** -> **WLAN** -> **Bridge Links** -> **Automatic Bridge Link Configuration**

After successful scanning, a selection of potential bridge partners is displayed in the scan list. In the **Action** column, click on **[Connect]** to connect the local bridge with this bridge. If the partners are connected with one another, the icon appears in the **Connected** column. The icon appears in the **Connected** column if the connection is active.

The **Wireless LAN** -> **WLAN** -> **Bridge Links** -> **Automatic Bridge Link Configuration** menu consists of the following fields.

Fields in the Automatic Bridge L ink Configuration menu

Field	Description
Bridge Link Description	Displays the name of the bridge link you configured.
Max. Scan Duration	Enter the maximum time in seconds for the scan. Possible values are `10` to `600`. The default value is `120`.
Action	Start the scan by clicking on **Scan**. If the antennas are installed correctly on both sides and LOS is free, the bridge finds available bridges and displays them in the following list. If the partner bridge cannot be found, check the line of sight and the antenna installation. Then carry out the **Scan** again. The partner should then be found.

Field	Description
Remote Link Description	Displays the name of the bridge link configured on the remote bridge.
Remote Device Name	Displays the name of the remote bridge.
Signal dBm	Displays the signal strength of the detected bridge link.
Remote MAC Address	Shows the MAC address of the remote bridge.
Remote Link Enabled	Displays the status of the link on the remote bridge.
Connected	Displays the status of the link on your bridge.
Action	You can change the status of the bridge link. The available actions are displayed in this field.

12.2 Administration

The **Wireless LAN** -> **Administration** menu contains basic settings for running your gateway as an access point (AP).

12.2.1 Basic Settings

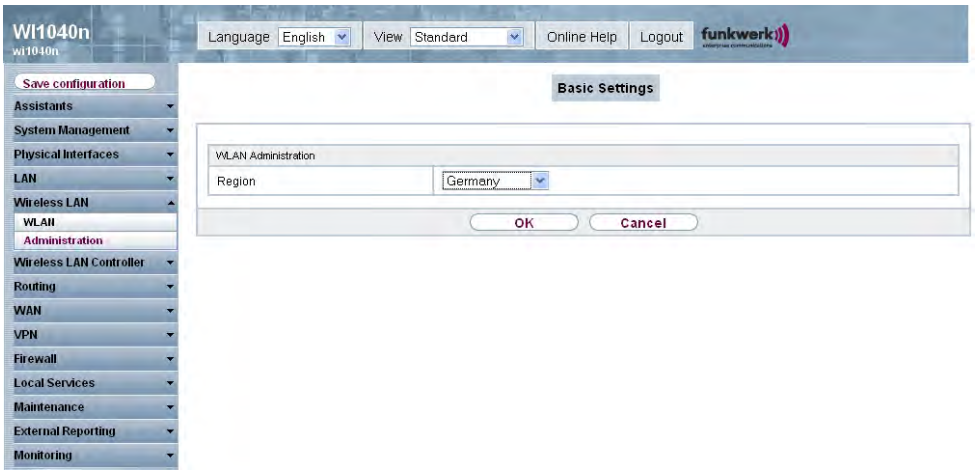


Fig. 76: **Wireless LAN** -> **Administration** -> **Basic Settings**

The **Wireless LAN** -> **Administration** -> **Basic Settings** menu consists of the following fields:

Fields in the Basic Settings WLAN Administration menu

Field	Description
Region	Select the country in which the access point is to be run. Possible values are all the countries configured on the device's wireless module. The range of channels available for selection (**Channel** in the **WLAN Wireless Modules** menu) changes depending on the country setting. The default value is `Germany`.

Chapter 13 Wireless LAN Controller

By using the wireless LAN controller, you can set up and manage a WLAN infrastructure with up to 24 access points (APs). The WLAN controller has a Wizard which assists you in the configuration of your access points. The system uses the CAPWAP protocol (Control and Provisioning of Wireless Access Points Protocol) for any communication between masters and slaves.

In smaller WLAN infrastructures with up to six APs, one of the AP's assumes the master function and manages the other AP's as well as itself. In larger WLAN networks a gateway, e.g. such as a **R1202**, assumes the master function and manages the AP's.

Provided the controller has "located" all of the APs in its system, each of these shall receive a new passport and configuration in succession, i.e. they are managed via the WLAN controller and can no longer be amended "externally".

With the **bintec WLAN controller** you can

- automatically detect individual access points (APs) and connect to a WLAN network
- Load the system software into the APs
- Load the configuration into the APs
- Monitor and manage APs

13.1 Wizard

The **Wizard** menu offers step-by-step instructions for the set up of a WLAN infrastructure. The Wizard guides you through the configuration.

When you select the Wizard you will receive instructions and explanations on the separate pages of the Wizard.

Note

We highly recommended that you use the Wizard when initially configuring your WLAN infrastructure.

13.1.1 Basic Setup

Here you can configure all of the various settings that you require for the actual wireless LAN controller.

The wireless LAN controller uses the following settings:

Region

Select the country in which the wireless controller is to be operated.

Note: The range of channels that can be used varies depending on the country setting.

Interface

Select the interface to be used for the wireless controller.

DHCP Server

Select whether an external DHCP server shall assign IP addresses to the APs or if your device should be used as the DHCP server. For an internal DHCP server, CAPWAP option 138 is enabled in order to allow communication between the master and slaves.

Note: Make sure that option 138 is enabled when using an external DHCP server.

If, for example, you want to use a bintec gateway as a DHCP server, click on the **Add** button in the **DHCP Options** field in the FCI menu of the device under **Local Services** -> **DHCP Server** -> **DHCP Pool**-> **New** -> **Advanced Settings** . In **Option** select *CAPWAP Controller* and enter the IP address of the WLAN controller in the **Value** field.

IP Address Range

If the IP addresses are to be assigned internally, you must enter the start and end IP address of the desired range.

Note: If you click on **Continue**, a warning appears which informs you that continuing will overwrite the wireless LAN controller configuration. Clicking on **OK** means that you agree with this and wish to continue with the configuration.

13.1.2 Wireless Radio Profiles

Select which frequency band your WLAN controller shall use.

If the *2.4 GHz Radio Profile* is set then the 2.4 GHz frequency band is used.

If the *5 GHz Radio Profile* is set then the 5 GHz frequency band is used.

13.1.3 Wireless Networks

All of the configured wireless networks (VSS) are displayed in the list. At least one wireless network (VSS) is set up. This entry cannot be deleted.

Click on to edit an existing entry.

You can also delete entries with the aid of .

With **Add**, you can create new entries. You can create up to eight wireless networks (VSS) for a wireless module.

Note: If you wish to use the default wireless network that is set up, then you must at least change the **Preshared Key** parameters. Otherwise you will be prompted.

13.1.3.1 Change or add wireless networks

Click on to edit an existing entry.

With **Add**, you can create new entries.

The following parameters are available

Network Name (SSID)

Enter the name of the wireless network (SSID).

Enter an ASCII string with a maximum of 32 characters.

Also select whether the **Network Name (SSID)** is to be transmitted with the *Visible* option.

Security Mode

Select the security mode (encryption and authentication) for the wireless network.

Note: *WPA-Enterprise* refers to 802.11x.

Transmit Key

Enter a transmission key for **Security Mode** = *WEP 40* or *WEP 104* .

Select one of the keys configured in **WEP Key <1 - 4>** as the default key.

WEP Key 1 - 4

Enter a WEP key for **Security Mode** = *WEP 40* or *WEP 104* .

Note: Enter a character string with the right number of characters for the selected WEP mode. For *WEP 40* you need a string of 5 characters, *WEP 104* 13 characters. For example *hello* for *WEP 40*, *funkwerk-wep1* for *WEP 104*.

WPA Mode

Depending on whether you wish to use WPA or WPA 2 or both, select for **Security Mode** = *WPA-PSK* or *WPA-Enterprise* .

WPA Cipher

Depending on which encryption you wish to use with WPA, select for **Security Mode** = *WPA-PSK* or *WPA-Enterprise* and for **WPA Mode** = *WPA* or *WPA and WPA2* .

WPA2 Cipher

Depending on which encryption you wish to use with WPA2, select for **Security Mode** = *WPA-PSK* or *WPA-Enterprise* and for **WPA Mode** = *WPA2* or *WPA and WPA2* .

Preshared Key

Enter the WPA password for **Security Mode** = *WPA-PSK* .

Enter an ASCII string with 8 - 63 characters.

Note: Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorised access!

RADIUS Server

You can control access to a wireless network via a RADIUS server.

With **Add**, you can create new entries.

Enter the IP address and the password of the desired RADIUS server.

EAP Preauthentification

For **Security Mode** = *WPA-Enterprise*, select whether the EAP preauthentification function is to be set as *Activated*. This function tells your device that WLAN clients, which are already connected to another access point, can first carry out 802.1x authentication as soon as they are within range. Such WLAN clients can then simply connect over the existing network connection with your device.

VLAN

Select whether the VLAN segmentation is to be used for this wireless network.

If you wish to use VLAN segmentation, enter a value between *1* and *4094* in the input field in order to identify the VLAN.

Note: Before you continue, please ensure that all access points that the WLAN controller shall manage are correctly wired and switched on.

13.1.4 Start automatic installation

You will see a list of all detected access points.

If you wish to change the settings of a detected AP, click on in the corresponding entry.

You will see the settings for all selected access points. You can change these settings.

The following parameters are available:

Location

Displays the stated locality of the AP. You can enter another locality.

Active Radio Profile

Displays the wireless module profile that is currently selected. You can select another wireless module profile from the list if several wireless module profiles are set up.

Assigned Wireless Networks (VSS)

Displays the wireless networks that are currently assigned.

Operation Mode

Select whether the device is to be operated in *Access Point* mode or in *Standard* mode. The *Standard* setting uses the value that you have selected in the corresponding **Radio Profile**.

Channel

Displays the channel that is assigned. You can select an alternative channel.

The number of channels you can selected depends on the country setting. Please consult the data sheet for your device.

Note: Configuring the network name (SSID) in Access Point mode means that wireless networks can be logically separated from each other, but they can still physically interfere with each other if they are operating on the same or closely adjacent wireless channels. So if you are operating two or more radio networks close to each other, it is advisable to allocate the networks to different channels. Each of these should be spaced at least four channels apart, as a network also partially occupies the adjacent channels.

In the case of manual channel selection, please make sure first that the APs actually support these channels.

Transmit Power

Displays the transmission power in dBm. You can select another transmission power.

By pressing **OK** you apply the settings in the **Access Point Settings** window.

Select the access points that your WLAN controller shall manage. In the **Manage** column, click on the desired entries or click on **Select All** in order to select all entries.

Click on **Start** in order to install the WLAN and automatically assign the frequencies.

Note: If there are not enough licences available, the message "The maximum number of slave access points that can be supported has been exceeded". Please check your licences. If this message is displayed then you should obtain additional licences if appropriate.

During the installation of the WLAN and the allocation of frequencies, on the messages displayed you will see how far the installation has progressed. The display is continuously updated.

Provided that non-overlapping wireless channels are located for all access points, the configuration that is set in the Wizard is transferred to the access points.

When the installation is complete, you will see a list of the **Managed** access points.

13.2 Controller Configuration

In this menu, you make the basic settings for the wireless LAN controller.

13.2.1 General

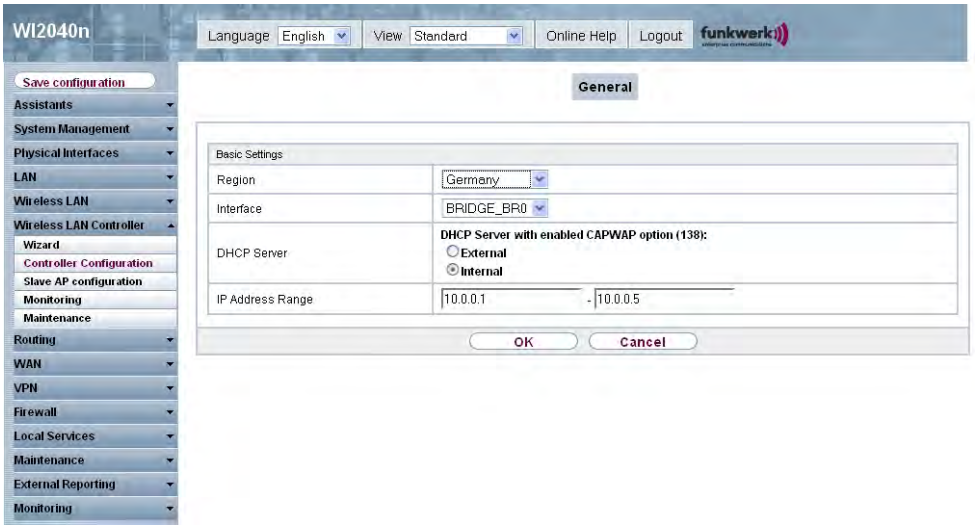


Fig. 77: **Wireless LAN Controller** -> **Controller Configuration** -> **General**

The **Wireless LAN Controller** -> **Controller Configuration** -> **General** menu consists of the following fields:

Fields in the General Basic Settings menu

Field	Description
Region	Select the country in which the wireless LAN controller is to be operated. Possible values are all the countries configured on the device's wireless module. The range of channels that can be used varies depending on the country setting. The default value is `Germany`.
Interface	Select the interface to be used for the wireless controller.
DHCP Server	Select whether an external DHCP server shall assign IP addresses to the APs or if your device should be used as the DHCP server. For an internal DHCP server, CAPWAP option 138 is active in order to allow communication between the master

Field	Description
	and slaves. Note: Make sure that option 138 is active when using an external DHCP server. Possible values: • *DHCP Server with enabled CAPWAP option (138): External* (default value): An external DHCP server with active CAPWAP option 138 assigns the IP addresses to the APs. • *DHCP Server with enabled CAPWAP option (138): Internal*: Your device, on which the CAPWAP option 138 is active, assigns the IP addresses to the APs.
IP Address Range	Only for **DHCP Server** = *DHCP server with enabled CAPWAP option (138): Internal* Enter the start and end IP address of the range. These IP addresses and your device must originate from the same network.

13.3 Slave AP Configuration

In this menu, you will find all of the settings that are required to manage the slave access points.

13.3.1 Slave Access Points

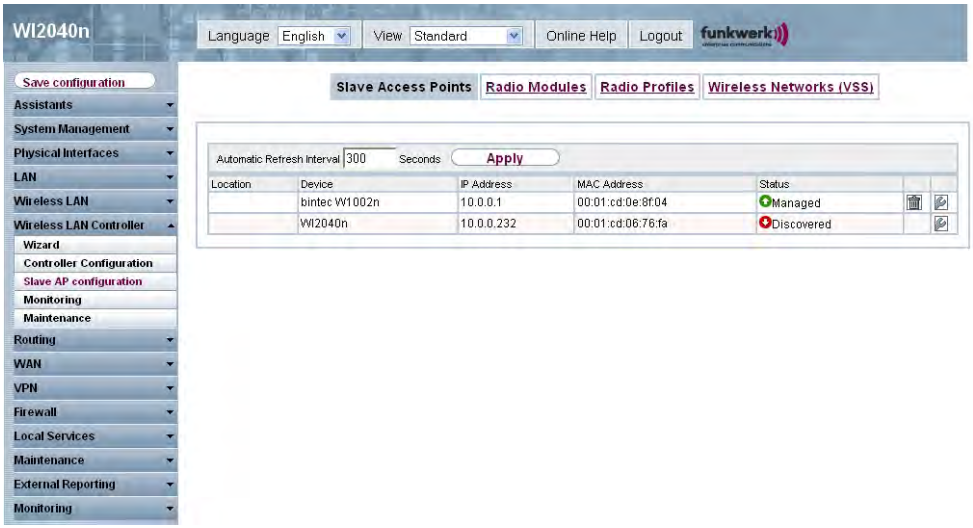


Fig. 78: **Wireless LAN Controller** -> **Slave AP configuration** -> **Slave Access Points**

In the **Wireless LAN Controller** -> **Slave AP configuration** -> **Slave Access Points** menu, a list of all located APs is displayed with help from the Wizard.

For each access point you will see an entry with a parameter set (**Location**, **Device**, **IP Address**, **MAC Address**, **Status**).

Possible values for Status:

Status	Meaning
Discovered	The AP has received an IP address via the DHCP and has communicated this to the controller via option 138. The controller has prompted the required parameters from the AP.
Initialise	The WLAN controller and the APs "communicate" via CAPWAP. The configuration is transferred and enabled to the APs.
Managed	The AP is set to "Managed" status. The controller has sent a configuration to the AP and has enabled this. The AP is managed centrally from the controller and cannot be configured via the FCI.
No licence available	The AP does not have a WLAN controller licence.
Off	The AP is either administratively disabled or switched off or has its power supply cut off etc.

13.3.1.1 Edit

Choose the icon to edit existing entries.

You can also delete entries with the aid of . If you have deleted APs, these will be located again but shall not be configured.

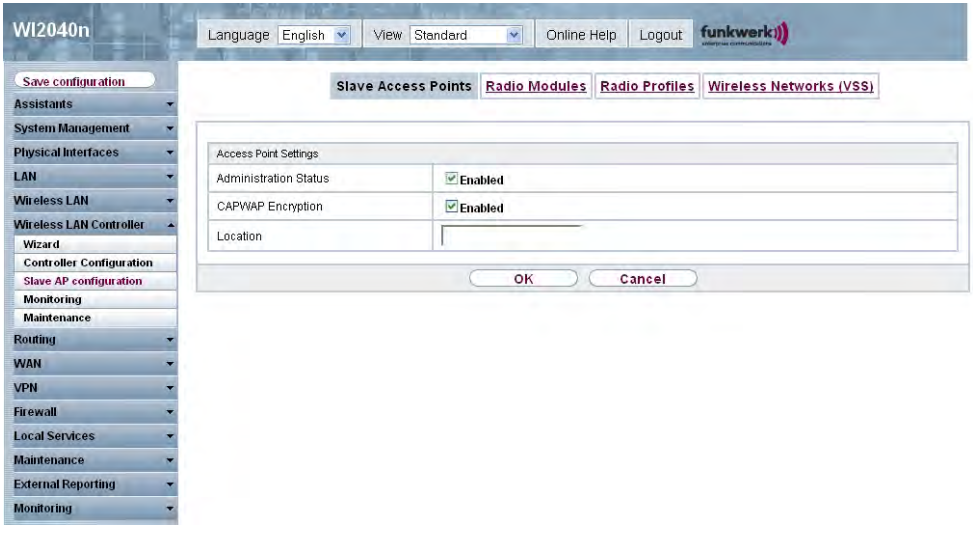


Fig. 79: **Wireless LAN Controller** -> **Slave AP Configuration** -> **Slave Access Points** ->

The **Wireless LAN Controller** -> **Slave AP Configuration** -> **Slave Access Points** -> menu consists of the following fields:

Fields in the Slave Access Points Access Point Settings menu

Field	Description
Administrative Status	Select whether the selected AP is to be managed from the WLAN controller. The function is activated by choosing *Enabled*. The function is enabled by default. You can disconnect the AP from the WLAN controller and therefore remove it from your WLAN infrastructure by disabling the function. The AP then receives the *Located* status but is no longer *Managed*.

Field	Description
CAPWAP Encryption	Select whether communication between the master and slaves is to be encrypted. The function is activated by choosing *Enabled*. The function is enabled by default. You can override the encryption in order to view the communication for debugging purposes.
Location	Displays the stated locality of the AP. You can enter another locality.

13.3.2 Radio Modules

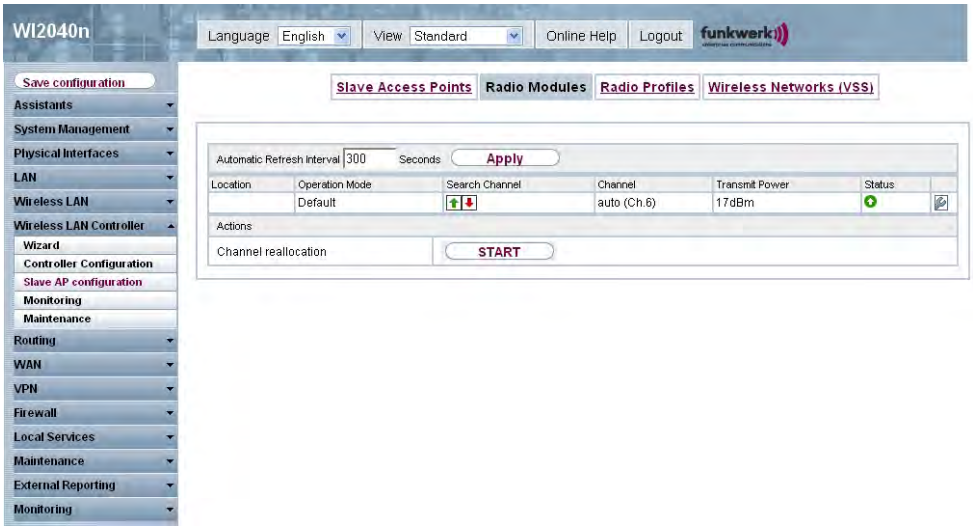


Fig. 80: **Wireless LAN Controller** -> **Slave AP Configuration** -> **Radio Modules**

In the **Wireless LAN Controller** -> **Slave AP Configuration** -> **Radio Modules** menu, an overview of all available wireless modules is displayed.

For each wireless module you will see an entry with a parameter set (**Location**, **Operation Mode**, **Channel Search**, **Channel**, **Transmission Power** , **Status**).

Note

For devices with two wireless modules, two entries are displayed in the overview.

Click on the **Start** button under **Channel Reallocation** in order to reassign any assigned channels, e.g. when a new access point has been added.

13.3.2.1 Edit

Choose the icon to edit existing entries.

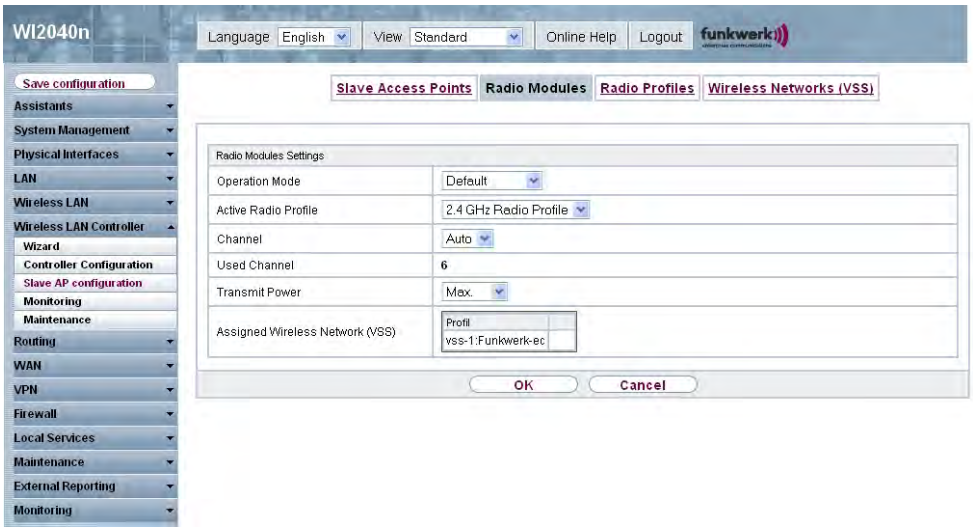


Fig. 81: **Wireless LAN Controller** -> **Slave AP Configuration** -> **Radio Modules** ->

The **Wireless LAN Controller** -> **Slave AP Configuration** -> **Radio Modules** -> menu consists of the following fields:

Fields in the Radio Modules Radio Modules Settings menu

Field	Description
Operation Mode	Displays the mode in which the wireless module is to be operated. You can change the mode. Possible values: • `Off` (default value) The wireless module is not active. • `Access Point`: The wireless module is used as an access point in your network. • `Default`: Uses the setting that was defined in the wireless module profile.
Active Radio Profile	Displays the wireless module profile that is currently selected.

Field	Description
	You can select another wireless module profile from the list if several wireless module profiles are set up.
Channel	Displays the channel that is assigned. You can select another channel. The number of channels you can selected depends on the country setting. Please consult the data sheet for your device. Access Point mode Configuring the network name (SSID) in Access Point mode means that wireless networks can be logically separated from each other, but they can still physically interfere with each other if they are operating on the same or closely adjacent wireless channels. So if you are operating two or more radio networks close to each other, it is advisable to allocate the networks to different channels. Each of these should be spaced at least four channels apart, as a network also partially occupies the adjacent channels. In the case of manual channel selection, please make sure first that the APs actually support these channels. Possible values (according to the selected wireless module profile): • For **Frequency Band** = *2.4 GHz In/Outdoor* Possible values are *1* to *13* and *Auto* (default value). • For **Frequency Band** = *5 GHz Indoor* Possible values are *36*, *40*, *44*, *48* and *Auto* (default value) • For **Operation Band** = *5 GHz In/Outdoor* and *5 GHz Outdoor* and *5.8 GHz Outdoor* Only the *Auto* option is possible here.
Used Channel	Only for managed APs. Displays the channel that is currently in use.
Transmit Power	Displays the transmission power. You can select another transmission power.

Field	Description
	Possible values: • `Max.` (default value): The maximum antenna power is used. • `5 dBm` • `8 dBm` • `11 dBm` • `14 dBm` • `16 dBm`
Assigned Wireless Networks (VSS)	Displays the wireless networks that are currently assigned.

13.3.3 Radio Profiles

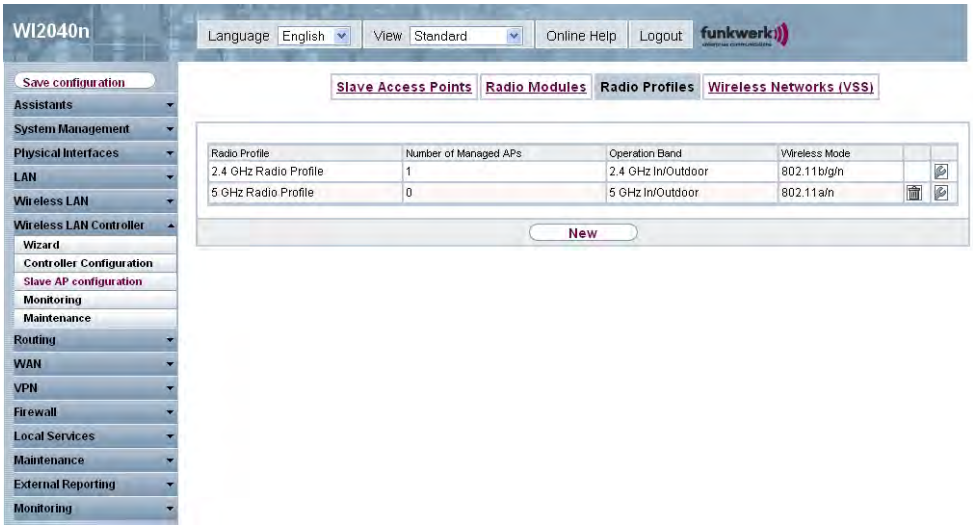


Fig. 82: **Wireless LAN Controller** -> **Slave AP Configuration** -> **Radio Profiles**

In the **Wireless LAN Controller** -> **Slave AP Configuration** -> **Radio Profiles** menu, an overview of all available wireless module profiles is displayed. A profile with 2.4 GHz and a profile with 5 GHz are created by default; the 2.4 GHz profile cannot be deleted.

For each wireless module profile you will see an entry with a parameter set (**Radio Profile**, **Number of Managed APs**, **Operation Band**, **Wireless Mode**).

13.3.3.1 Edit/New

Choose the icon to edit existing entries. Select the **New**button in order to create new wireless module profiles.

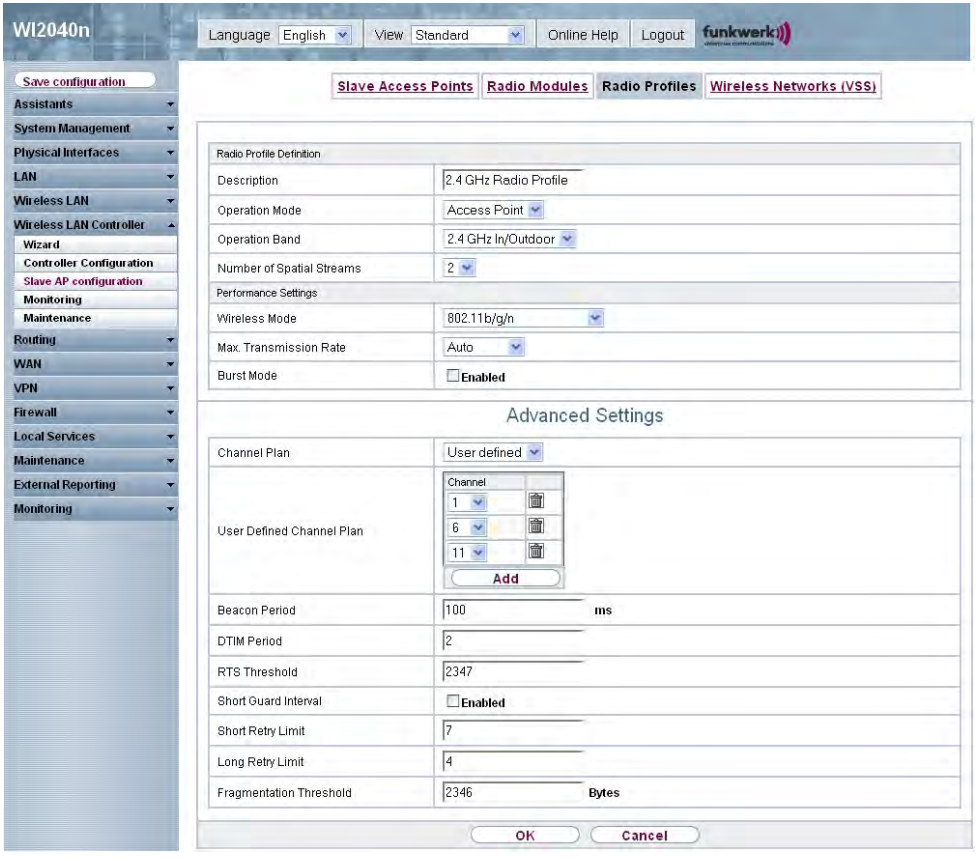


Fig. 83: **Wireless LAN Controller** -> **Slave AP Configuration** -> **Radio Profiles** ->**/New**

The **Wireless LAN Controller** -> **Slave AP Configuration** -> **Radio Profiles** ->**/New** menu consists of the following fields:

Fields in the Radio Profiles Radio Profile Definition

Field	Description
Description	Enter the desired description of the wireless module profile.
Operation Mode	Define the mode in which the wireless module profile is to be operated.

Field	Description
	Possible values: • *Off* (default value) The wireless module profile is not active. • *Access Point*: Your device is used as an access point in your network.
Operation Band	Select the frequency band of the wireless module profile. Possible values: • *2.4 GHz In/Outdoor* (default value): Your device is operated at 2.4 GHz (mode 802.11b, mode 802.11g and mode 802.11n), inside or outside buildings. • *5 GHz Indoor*: Your device is operated at 5 GHz (mode 802.11a/h and mode 802.11n) inside buildings. • *5 GHz Outdoor*: Your device is operated at 5 GHz (mode 802.11a/h and mode 802.11n) outside buildings. • *5 GHz In/Outdoor*: Your device is operated at 5 GHz (mode 802.11a/h and mode 802.11n) inside or outside buildings. • *5.8 GHz Outdoor*: Only for so-called Broadband Fixed Wireless Access (BFWA) applications. The frequencies in the frequency range from 5755 MHz to 5875 MHz may only be used in conjunction with commercial offers for public network accesses and requires registration with the Federal Network Agency.
Bandwidth	Not for **Frequency Band** = *2.4 GHz In/Outdoor* Select how many channels are to be used. Possible values: • *20 MHz* (default value): One channel with 20 MHz bandwidth is used. • *40 MHz*: Two channels each with 20 MHz bandwidth are used. In the case one channel acts as a control channel and the other as an expansion channel.
Number of Spatial Streams	Select how many traffic flows are to be used in parallel. Possible values:

Field	Description
	• *2* (default value): Two traffic flows are used. • *1*: One traffic flow is used.

Fields in the Wireless Modules Performance Settings menu

Field	Description
Wireless Mode	Select the wireless technology that the access point is to use. For **Frequency Band** = *2,4 GHz In/Outdoor* Possible values: • *802.11 b/g/n*: Your device operates according to either 802.11b, 802.11g or 802.11n. • *802.11 g/n*: Your device operates according to either 802.11g or 802.11n. • *802.11 n*: Your device operates only according to 802.11n. • *802.11g*: The device operates only in accordance with 802.11g. 802.11b clients have no access. • *802.11b*: Your device operates only in accordance with 802.11b and forces all clients to adapt to it. • *802.11 mixed (b/g)*: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. • *802.11 mixed-long (b/g)*: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. Only a data rate of 1 and 2 mbps needs to be supported by all clients (basic rates). This mode is also needed for Centrino clients if connection problems occur. • *802.11 mixed-short (b/g)*: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. The following applies for mixed-short: The data rates 5.5 and 11 mbps must be supported by all clients (basic rates). For **Frequency Band** = *5 GHz Indoor* , *5 GHz Outdoor* , *5 GHz In/Outdoor* or *5.8 GHz Outdoor*

Field	Description
	Possible values: • *802.11 a/n*: Your device operates according to either 802.11a or 802.11n. • *802.11n*: Your device operates only according to 802.11n. • *802.11a*: The device operates only in accordance with 802.11a.
Max. Transmission Rate	Select the transmission speed. Possible values: • *Auto* (default value) The transmission speed is determined automatically. • *<Value>*: Depending on the setting for **Operation Band**, **Bandwidth**, **Number of spatial streams** and **Wireless Mode**, different whole values in mbps will be available for selection.
Burst Mode	Activate this function to increase the transmission speed for 802.11g through frame bursting. As a result, several packets are sent one after the other without a waiting period. This is particularly effective in 11b/g mixed operation. The function is activated with *Enabled*. The function is disabled by default. If problems occur with older WLAN hardware, this function should not be active.

The **Advanced Settings** menu consists of the following fields:

Fields in the Wireless Modules Advanced Settings menu

Field	Description
Channel Plan	Select the desired channel plan. The channel plan makes a preselection when a channel is selected. This ensures that no channels overlap, i.e. a distance of four channels is maintained between the channels used. This is useful if more access points are used with overlapping radio cells.

Field	Description
	Possible values: • *All*: All channels can be dialled when a channel is selected. • *Auto*: Depending on the region, operation band, wireless mode and bandwidth, the channels that have a distance of 4 channels are provided. • *User Defined*: You can select the desired channels yourself.
User Defined Channel Plan	Only for **Channel Plan** = *User-defined*. The currently selected channels are displayed here. By using **Add** you can add channels. If all available channels are displayed, you cannot add any more entries. You can also delete entries with the aid of .
Beacon Period	Enter the time in milliseconds between the sending of two beacons. This value is transmitted in Beacon and Probe Response Frames. Possible values are *1* to *65535*. The default value is *100*.
DTIM Period	Enter the interval for the Delivery Traffic Indication Message (DTIM). The DTIM field is a data field in transmitted beacons that informs clients about the window to the next broadcast or multicast transmission. If clients operate in power save mode, they come alive at the right time and receive the data. Possible values are *1* to *255*. The default value is *2*.
RTS Threshold	Here you can specify the data packet length threshold in bytes (1..2346) as of which the RTS/CTS mechanism is to be used. This makes sense if several clients that are not in each other's wireless range are run in one access point.

Field	Description
Short Guard Interval	Enable this function to reduce the guard interval (= time between transmission of two data symbols) from 800 ns to 400 ns.
Short Retry Limit	Enter the maximum number of attempts to send a frame of length less than or equal to the value defined in **RTS Threshold**. After this many failed attempts, the packet is discarded. Possible values are *1* to *255*. The default value is *7*.
Long Retry Limit	Enter the maximum number of attempts to send a data packet of length greater than the value defined in **RTS Threshold**. After this many failed attempts, the packet is discarded. Possible values are *1* to *255*. The default value is *4*.
Fragmentation Threshold	Enter the maximum size as of which the data packets are to be fragmented (i.e. split into smaller units). Low values are recommended for this field in areas with poor reception and in the event of radio interference. Possible values are *256* to *2346*. The default value is *2346*.

13.3.4 Wireless Networks (VSS)

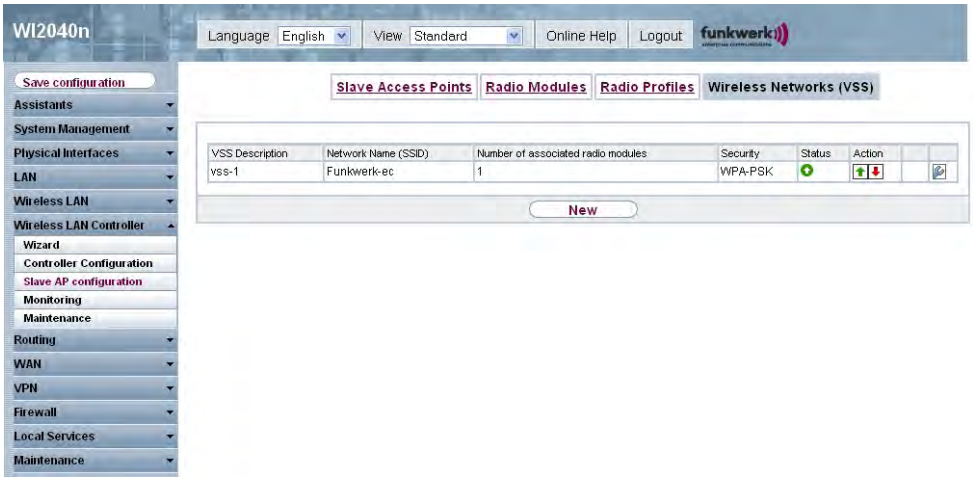


Fig. 84: **Wireless LAN Controller** -> **Slave AP Configuration** -> **Wireless Networks (VSS)**

In the **Wireless LAN Controller** -> **Slave AP Configuration** -> **Wireless Networks (VSS)** menu, an overview of all wireless networks that have been created is displayed. A wireless network is created by default.

For each wireless network (VSS) you will see an entry with a parameter set (**VSS Description**, **Network Name (SSID)**, **Number of associated radio modules**, **Security**, **Status**, **Action**).

13.3.4.1 Edit/New

Choose the icon to edit existing entries. Choose the **New** button to configure other wireless networks.

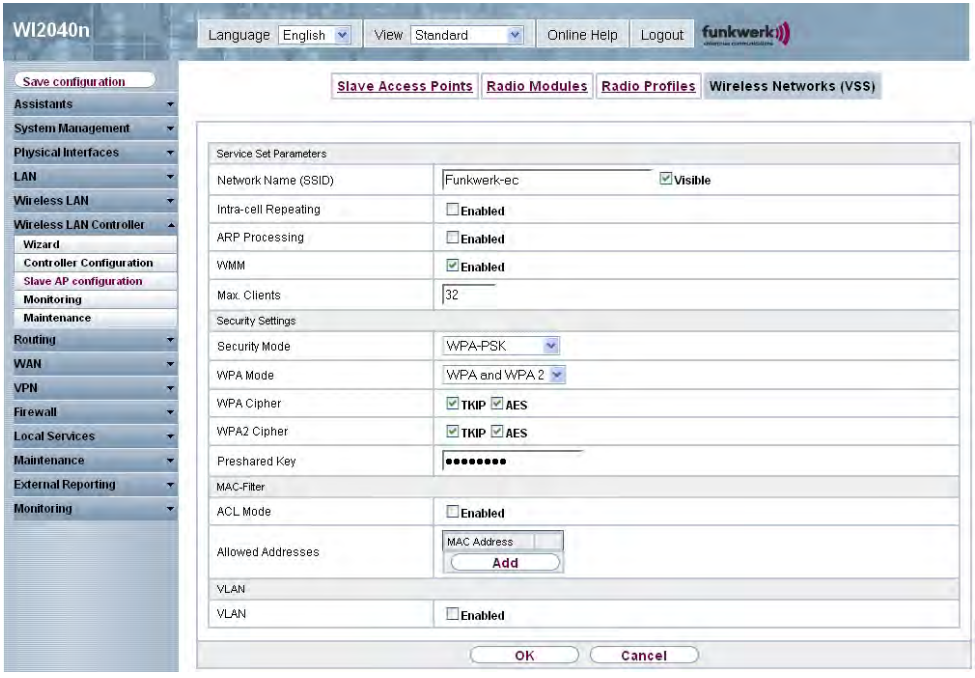


Fig. 85: **Wireless LAN Controller -> Slave AP Configuration -> Wireless Networks (VSS) ->/New**

The **Wireless LAN Controller -> Slave AP Configuration -> Wireless Networks (VSS) ->/New** menu consists of the following fields:

Fields in the Virtual Service Sets Service Set Parameters menu

Field	Description
Network Name (SSID)	Enter the name of the wireless network (SSID). Enter an ASCII string with a maximum of 32 characters. Also select whether the **Network Name (SSID)** is to be transmitted. The network name is shown by choosing *Visible*. It is visible by default.
Intra-cell Repeating	Select whether communication between the WLAN clients is to be permitted within a radio cell. The function is activated by choosing *Enabled*.

Field	Description
	The function is enabled by default.
ARP Processing	Select whether the ARP processing function should be enabled. The ARP data traffic is reduced in the network by the fact that ARP broadcasts that have been converted to ARP unicasts are forwarded to IP addresses that are known internally. Unicasts are quicker and clients with an enabled power save function are not addressed. The function is activated by choosing *Enabled*. The function is disabled by default. Make sure that ARP processing cannot be applied together with the MAC bridge function.
WMM	Select whether voice or video prioritisation via WMM (Wireless Multimedia) is to be activated for the wireless network so that optimum transmission quality is always achieved for time-critical applications. Data prioritisation is supported in accordance with DSCP (Differentiated Services Code Point) or IEEE802.1d. The function is activated by choosing *Enabled*. The function is enabled by default.
Max. Clients	Enter the maximum number of clients that can be connected to this wireless network (SSID) The maximum number of clients that can register with a wireless module depends on the specifications of the respective WLAN module. This number can be shared across all configured wireless networks. If the maximum number of clients is reached, no more new wireless networks can be created and a warning message will appear.

Fields in the Virtual Service Sets Security Settings menu

Field	Description
Security Mode	Select the security mode (encryption and authentication) for the wireless network. Possible values:

Field	Description
	• *Inactive* (default value): Neither encryption nor authentication • *WEP 40*: WEP 40 Bit • *WEP 104*: WEP 104 Bit • *WPA-PSK*: WPA Preshared Key • *WPA-Enterprise*: 802.11x
Transmit Key	Only if **Security Mode** = *WEP 40, WEP 104* Select one of the keys configured in **WEP Key <1 - 4>** as the default key. The default value is *Key 1*.
WEP Key 1-4	Only if **Security Mode** = *WEP 40* , *WEP 104* Enter the WEP key. Enter a character string with the right number of characters for the selected WEP mode. For *WEP 40* you need a string of 5 characters, *WEP 104* 13 characters. For example *hello* for *WEP 40*, *funkwerk-wep1* for *WEP 104*.
WPA Mode	Only if **Security Mode** = *WPA-PSK* and *WPA-Enterprise* Select whether you want to use WPA (with TKIP encryption) or WPA 2 (with AES encryption), or both. Possible values: • *WPA and WPA 2* (default value): WPA and WPA 2 can be used. • *WPA* : Only WPA is used. • *WPA 2* : Only WPA2 is used.
WPA Cipher	Only for **Security Mode** = *WPA-PSK* and *WPA-Enterprise* and for **WPA Mode** = *WPA* and *WPA and WPA2* Select the type of encryption you want to apply to WPA. Possible values: • *TKIP* (default value): TKIP is used.

Field	Description
	• *AES*: AES is used. • *AES and TKIP*: AES or TKIP is used.
WPA2 Cipher	Only for **Security Mode** = *WPA-PSK* and *WPA-Enterprise* and for **WPA Mode** = *WPA2* and *WPA and WPA2* Select the type of encryption you want to apply to WPA2. Possible values: • *AES* (default value): AES is used. • *TKIP* : TKIP is used. • *AES and TKIP*: AES or TKIP is used.
Preshared Key	Only if **Security Mode** = *WPA-PSK* Enter the WPA password. Enter an ASCII string with 8 - 63 characters. Note: Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorised access!
RADIUS Server	You can control access to a wireless network via a RADIUS server. With **Add**, you can create new entries. Enter the IP address and the password of the RADIUS server.
EAP Preauthentification	Only if **Security Mode** = *WPA-Enterprise* Select whether the EAP preauthentification function is to be activated. This function tells your device that WLAN clients, which are already connected to another access point, can first carry out 802.1x authentication as soon as they are within range. Such WLAN clients can then simply connect over the existing network connection with your device. The function is activated by choosing *Enabled*. The function is enabled by default.

Fields in the Virtual Service Sets MAC-Filter menu

Field	Description
ACL Mode	Select whether only certain clients are to be permitted for this wireless network. The function is activated by choosing *Enabled*. The function is disabled by default.
Allowed Addresses	Use **Add** to make entries and enter the MAC addresses (**MAC Address**) of the clients to be permitted.

Fields in the Wireless Networks (VSS) VLAN menu

Field	Description
VLAN	Select whether the VLAN segmentation is to be used for this wireless network. The function is activated by choosing *Enabled*. The function is disabled by default.
VLAN ID	Enter the number that identifies the VLAN. Possible values are *1* to *4094*.

13.4 Monitoring

This menu is used to monitor your WLAN infrastructure.

13.4.1 Active Clients

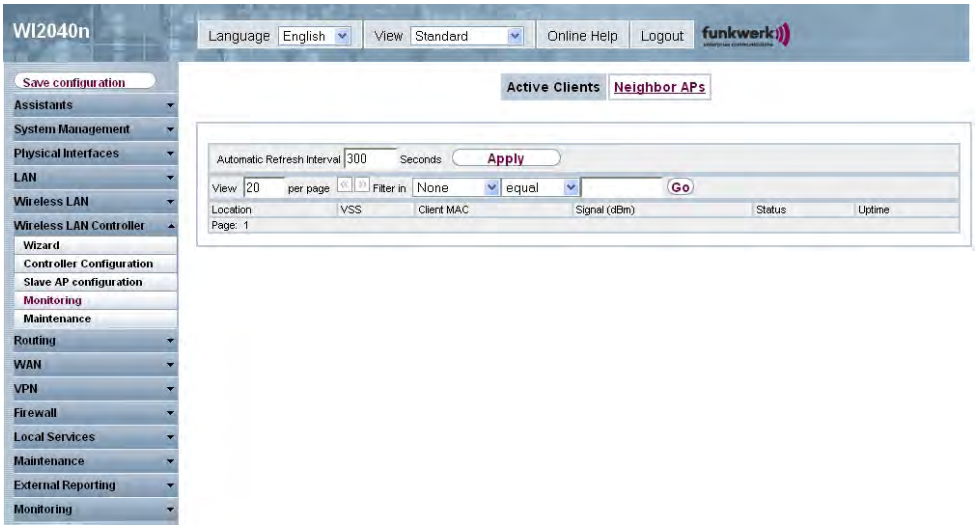


Fig. 86: **Wireless LAN Controller** -> **Monitoring** -> **Active Clients**

In the **Wireless LAN Controller** -> **Monitoring** -> **Active Clients** menu, the current values of all active clients are shown.

For each **Active Client** you will see an entry with a parameter set (**Location**, **VSS**, **Client MAC**, **Signal (dBm)**, **Status**, **Uptime**).

Possible values for Status

Status	Meaning
Open	The client is no longer in a valid status.
Logon	The client has just logged on with the WLAN controller.
Logged on	The client has logged on with the WLAN controller.
Authentication	The client is in the process of being authenticated.
Authenticated	The client is authenticated.

13.4.2 Neighbor APs

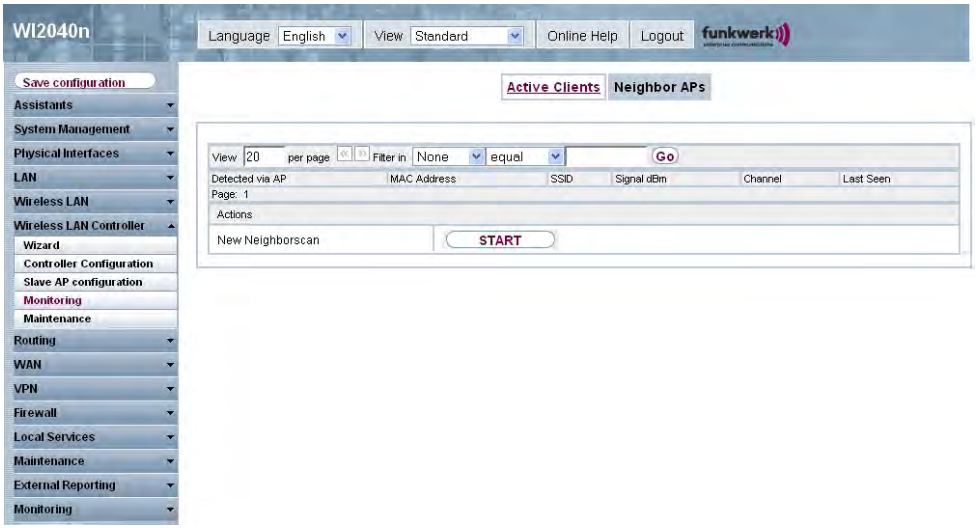


Fig. 87: **Wireless LAN Controller** -> **Monitoring** -> **Neighbor APs**

In the **Wireless LAN Controller** -> **Monitoring** -> **Neighbor APs** menu, all neighbouring APs that are located during the scan are displayed.

For each neighbouring AP you will see an entry with a parameter set (**Detected via AP**, **MAC Address**, **SSID**, **Signal (dBm)**, **Channel**, **Last Seen**; under **Detected via AP** you will see the locality of the respective device).

Click on **Start** under **New Neighborscan** in order to scan for neighbouring APs again. You will receive a warning that the wireless modules of the access points must also be disabled for a certain period of time. When you start the process with **OK** , a progress bar is displayed. The located AP display is updated every ten seconds.

13.5 Maintenance

This menu is used for the maintenance of your managed APs.

13.5.1 Firmware Maintenance

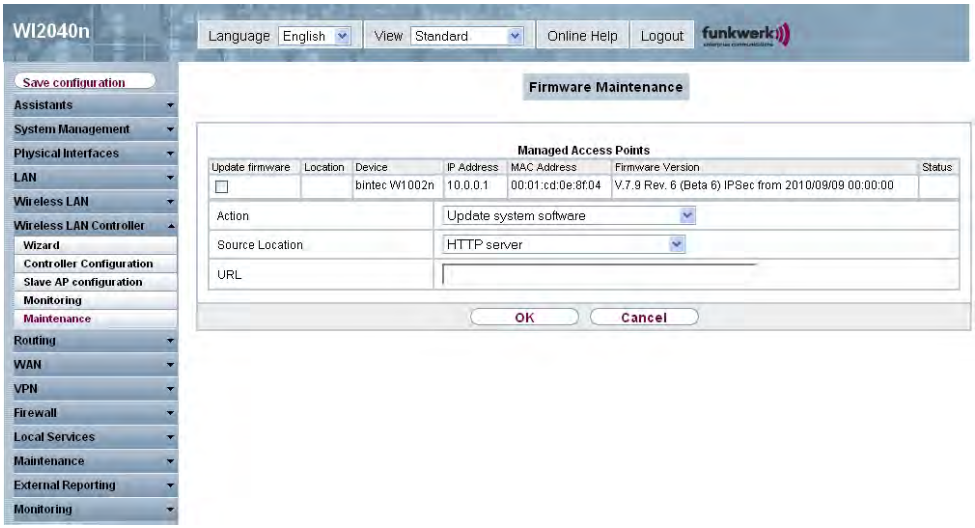


Fig. 88: **Wireless LAN Controller** -> **Maintenance** -> **Firmware Maintenance**

In the **Wireless LAN Controller** -> **Maintenance** -> **Firmware Maintenance** a list of all **Managed Access Points** is displayed.

For each managed AP you will see an entry with a parameter set (**Update firmware**, **Location**, **Device**, **IP Address**, **MAC Address**, **Firmware Version**, **Status**).

Possible values for Status

Status	Meaning
Image already exists	The software image already exists; no update is required.
Errors	An error has occurred.
In progress	The operation is currently in progress.
Complete	The update is complete.

The **Wireless LAN Controller** -> **Maintenance** -> **Firmware Maintenance** consists of the following fields:

Fields in the Firmware Maintenance menu

Field	Description
Action	Select the action you wish to execute. After each task, a window is displayed showing the other steps

Field	Description
	that are required. Possible values: • *Update system software*: You can also start an update of the system software. • *Save configuration with state information*: You can save a configuration which contains the AP status information.
Source Location	Select the source for the action. Possible values: • *HTTP server* (default value): The file is stored respectively on a remote server specified in the **URL**. • *Current software from Funkwerk server*: The file is on the official Funkwerk update server. (Only for **Action** = *Update system software*) • *TFTP Server*: The file is stored respectively on a TFTP server specified in the **URL**.
URL	Only for **Source** = *HTTP server* or *TFTP server* Enter the URL of the update server from which the system software file is loaded or on which the configuration file is saved.

Chapter 14 Routing

14.1 Routes

Default Route

With a default route, all data is automatically forwarded to one connection if no other suitable route is available. If you set up access to the Internet, you must configure the route to your Internet Service Provider (ISP) as a default route. If, for example, you configure a corporate network connection, only enter the route to the head office or branch office as a default route if you do not configure Internet access over your device. If, for example, you configure both Internet access and a corporate network connection, enter a default route to the ISP and a network route to the head office. You can enter several default routes on your device, but only one default route can be active at any one time. If you enter several default routes, you should make sure the values for **Metric** are different.

14.1.1 IP Routes

In the **Routing** -> **Routes** -> **IP Routes** menu a list of all configured routes is shown.

14.1.1.1 Edit/New

Choose the icon to edit existing entries. Choose the **New** button to create routes.

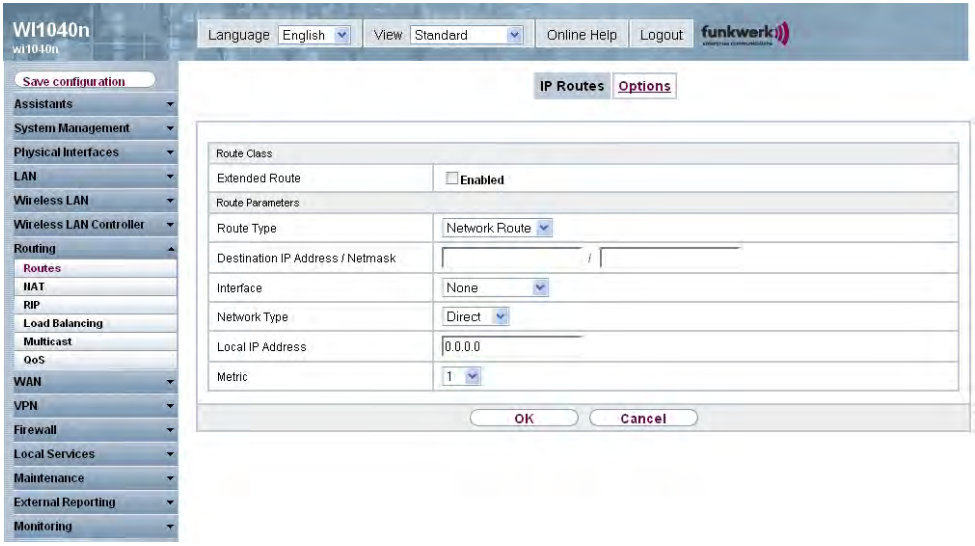


Fig. 89: **Routing** -> **Routes** -> **IP Routes**-> **New** *with* **Extended Route** = `Not activated`

If the `Extended Route` option is selected for **Route Class**, an extra configuration section opens.

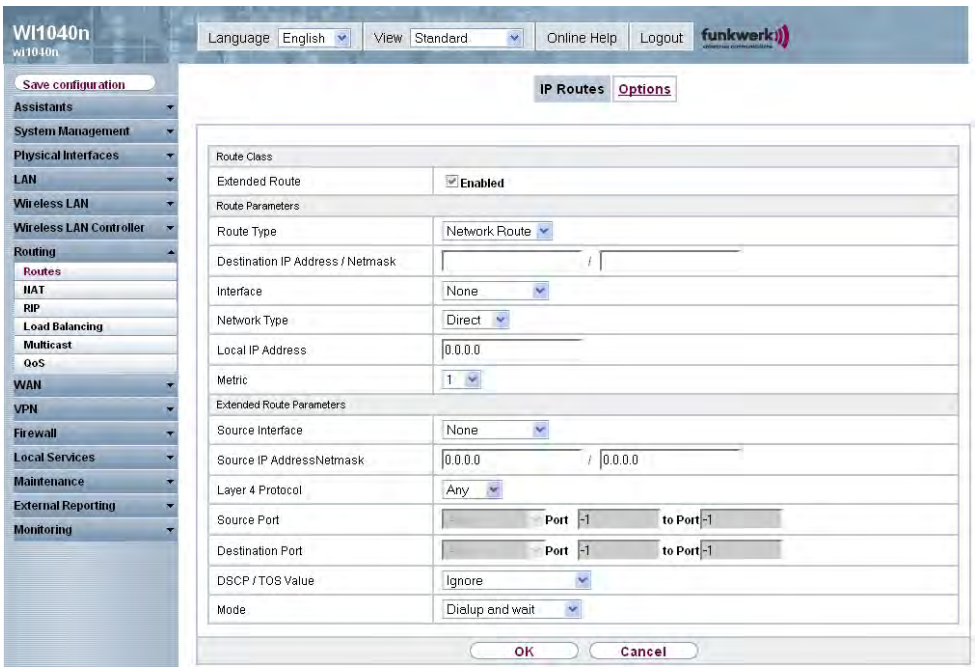


Fig. 90: **Routing** -> **Routes** -> **IP Routes**-> **New** *with* **Extended Route** = `Activated`

The **Routing** -> **Routes** -> **IP Routes**-> **New** menu consists of the following fields:

Fields in the IP Routes Route Class menu

Field	Description
Extended Route	Select whether the route is to be defined with extended parameters. If the function is active, a route is created with extended routing parameters such as source interface and source IP address, as well as protocol, source and destination port, type of service (TOS) and the status of the device interface. The function is activated by choosing *Enabled*. The function is disabled by default.

Fields in the IP Routes Route Parameters menu

Field	Description
Route Type	Select the type of route. Possible values: • *Network Route* (default value): Route to a network. • *Default Route* : Is used if no other suitable route is available. • *Host Route* : Route to a single host.
Destination IP Address / Netmask	Only if **Route Type** *Host Route* or *Network Route* Enter the IP address of the destination host. If **Route Type** = *Network Route* also enter the netmask in the second field. If no entry is made, your device uses a default netmask.
Interface	If necessary, enter the interface to be used for this route.
Network Type	Not for **Route Type** = *Standard Route* Also select the network type. Possible values: • *Direct* (default value): • in the LAN: You define another IP address for the interface.

Field	Description
	• in the WAN: You define a route without a transit network. • *Indirect*: • in the LAN: You define a gateway route. • in the WAN: You define a route with a transit network.
Local IP Address	Only for **Network Type** = *Direct*. Enter the IP address of the gateway to which your device is to forward the IP packets.
Gateway	Only for **Network Type** = *Indirect*. Enter the IP address of the host to which your device is to forward the IP packets.
Metric	Select the priority of the route. The lower the value, the higher the priority of the route. Value range from *0* to *15*, The default value is *1*.

Fields in the IP Routes Extended Route Parameters menu

Field	Description
Source Interface	Select the interface over which the data packets are to reach the device. The default value is *None*
Source IP Address / Netmask	Enter the IP address and netmask of the source host or source network.
Layer 4 Protocol	Select a protocol. Possible values: *ICMP* , *TCP* , *UDP* , *GRE* , *ESP* , *AH* , *OSPF* , *L2TP*, *Any* . The default value is *Any*
Source Port	Only if **Layer 4 Protocol** = *TCP* or *UDP*. Enter the source port.

Field	Description
	First select the port number range. Possible values: • *Any* (default value): The route is valid for all port numbers. • *Single*: Enables the entry of a port number. • *Range*: Enables the entry of a range of port numbers. • *Privileged*: Entry of privileged port numbers: 0 ... 1023. • *Server*: Entry of server port numbers: 5000 ... 32767. • *Clients 1*: Entry of client port numbers: 1024 ... 4999. • *Clients 2*: Entry of client port numbers: 32768 ... 65535. • *Not privileged*: Entry of unprivileged port numbers: 1024 ... 65535. Enter the appropriate values for the individual port or start port of a range in **Port** and, for a range, the end port in **to Port**.
Destination Port	Only if **Layer 4 Protocol** = *TCP* or *UDP*. Enter the destination port. First select the port number range. Possible values: • *Any* (default value): The route is valid for all port numbers. • *Single*: Enables the entry of a port number. • *Range*: Enables the entry of a range of port numbers. • *Privileged*: Entry of privileged port numbers: 0 ... 1023. • *Server*: Entry of server port numbers: 5000 ... 32767. • *Clients 1*: Entry of client port numbers: 1024 ... 4999. • *Clients 2*: Entry of client port numbers: 32768 ... 65535. • *Not privileged*: Entry of unprivileged port numbers: 1024 ... 65535. Enter the appropriate values for the individual port or start port of a range in **Port** and, for a range, the end port in **to Port**.
DSCP / TOS Value	Select the Type of Service (TOS).

Field	Description
	Possible values: • *Ignore* (default value): The type of service is ignored. • *DSCP*: Relates to a Differentiated Services Code Point to RFC 3260. • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. Enter the relevant value for *DSCP*, *TOS Binary Value* and *TOS Decimal Value*.
Mode	Select when the interface defined in **Route Parameters** -> **Interface** is to be used. Possible values: • *Dialup and wait* (default value): The route can be used if the interface is "up". If the interface is "dormant", then dial and wait until the interface is "up". • *Authoritative* : The route can always be used. • *Dialup and continue*: The route can be used if the interface is "up". If the interface is "dormant", then select and use the alternative route (rerouting) until the interface is "up". • *Never dialup*: The route can be used if the interface is "up". • *Always dialup*: The route can be used if the interface is "up". If the interface is "dormant", then dial and wait until the interface is "up". In this case, an alternative interface with a poorer metric is used for routing until the interface is "up".

14.1.2 Options

Back Route Verify

The term Back Route Verify describes a very simple but powerful function. If a check is activated for an interface, incoming data packets are only accepted over this interface if outgoing response packets are routed over the same interface. You can therefore prevent the acceptance of packets with false IP addresses - even without using filters.

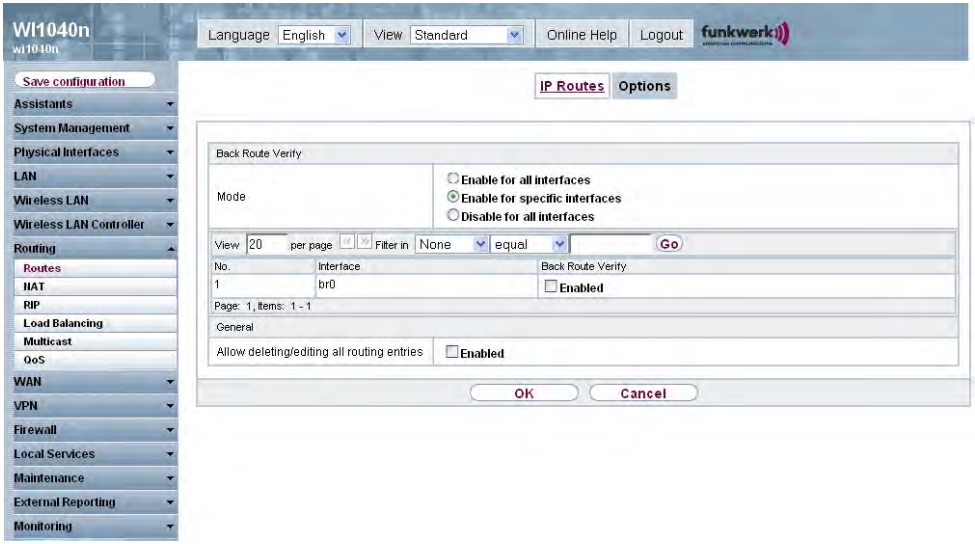


Fig. 91: **Routing** -> **Routes** -> **Options**

The **Routing** -> **Routes** -> **Options** menu consists of the following fields:

Fields in the Options Back Route Verify menu

Field	Description
Mode	Select how the interfaces to be activated for Back Route Verify are to be specified. Possible values: • *Enable for all Interfaces*: Back Route Verify is activated for all interfaces. • *Enable for specific interfaces* (default value): A list of all interfaces is displayed in which Back Route Verify is only enabled for specific interfaces. • *Disable for all interfaces*: Back Route Verify is disabled for all interfaces.
No.	Only for **Mode** = *Enable for specific interfaces* Displays the serial number of the list entry.
Interface	Only for **Mode** = *Enable for specific interfaces* Displays the name of the interface.

Field	Description
Back Route Verify	Only for **Mode** = *Enable for specific interfaces* Select whether *Return Route Checking* is to be enabled for this interface. The function is activated with *Enabled*. By default, the function is deactivated for all interfaces.

Fields in the Options General menu

Field	Description
Allow deleting/editing all routing entries	Define whether all the routes entered on your device can be edited and deleted in the **Routing** -> **Routes** -> **Routes** menu. The function is activated with *Enabled*. By default, the function is deactivated for all interfaces.

14.2 NAT

Network Address Translation (NAT) is a function on your device for defined conversion of source and destination addresses of IP packets. If NAT is activated, IP connections are still only allowed by default in one direction, outgoing (forward) (= protective function). Exceptions to the rule can be configured (in *NAT Configuration* on page 218).

14.2.1 NAT Interfaces

In the **Routing** -> **NAT** -> **NAT Interfaces** menu, a list of all NAT interfaces is shown.

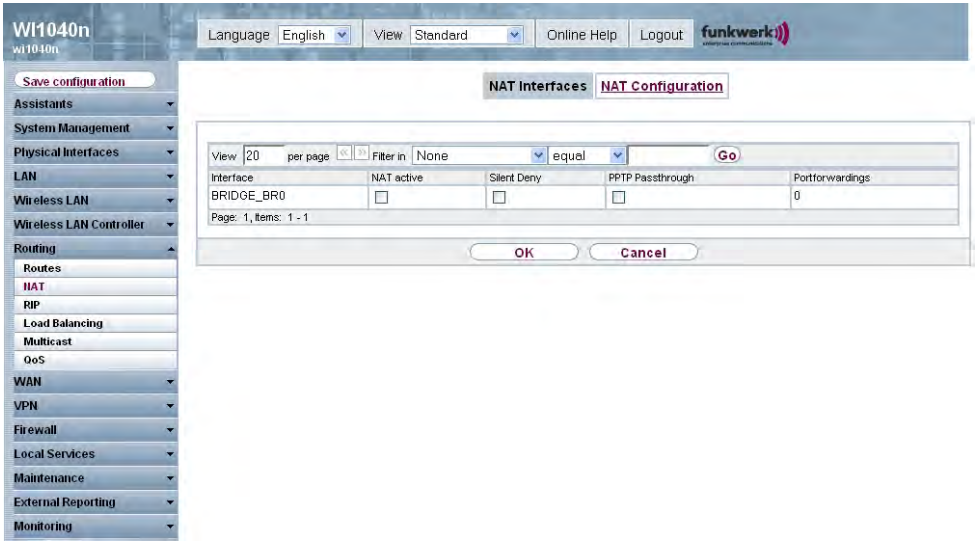


Fig. 92: **Routing -> NAT ->NAT Interfaces**

For each NAT interface, you can select the options *NAT Active*, *Silent Deny* and *PPTP Passthrough*.

In addition, *Portforwardings* displays how many port forwarding rules were configured for this interface.

Options in the menu NAT Interfaces

Field	Description
NAT active	Select whether NAT is to be activated for the interface. The function is disabled by default.
Silent Deny	Select whether IP packets are to be silently denied by NAT. If this function is deactivated, the sender of the denied IP packet is informed by means of an ICMP or TCP RST message. The function is disabled by default.
PPTP Passthrough	Select whether the setup and operation of several simultaneous, outgoing PPTP connections from hosts in the network are also to be permitted if NAT is activated. The function is disabled by default. If **PPTP Passthrough** is enabled, the device itself cannot be configured as a tunnel endpoint.

Field	Description
Portforwardings	Shows the number of portforwarding rules configured in **Routing** -> **NAT** -> **Portforwarding**.

14.2.2 NAT Configuration

In the **Routing** -> **NAT** -> **NAT Configuration** menu you can exclude data from NAT in a simple and convenient manner. You can configure var- ious NAT methods. You can determine how an external host establishes a con- nection to an internal host (refer to RFC 3489).

14.2.2.1 New

Choose the **New** button to set up NAT.

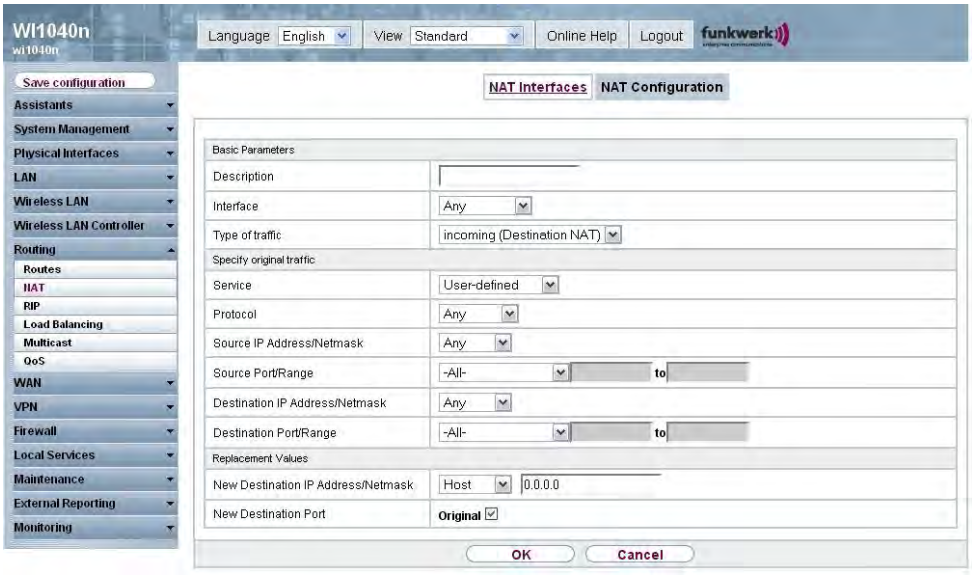


Fig. 93: **Routing** -> **NAT** ->**NAT Configuration** -> **New**

The **Routing** -> **NAT** -> **NAT Configuration** -> **New** menu consists of the following fields:

Fields in the NAT Configuration Basic Parameters menu

Field	Description
Description	Enter a description for the NAT Configuration.
Interface	Select the interface for which NAT is to be configured.

Field	Description
Type of traffic	Select the type of data traffic for which NAT is to be configured. Possible values: • *incoming (Destination NAT)* (default value): The data traffic that comes from outside. • *outgoing (Source NAT)* : The data traffic that goes outside. • *exclusive (Without NAT)* : The data traffic that is excluded from NAT.
NAT method	Only for **Type of traffic** = *outgoing (Source NAT)*. Select the NAT method for outgoing data traffic. The starting point for choosing the NAT method is a NAT scenario where an "internal" source host has initialized an IP connection to an "external" destination host over a NAT interface and where an internal valid source address and an internal valid source port are mapped to an external valid source address and an external valid source port. Possible values: • *full-cone*(only UDP): Any external host may send IP packets to the initializing source address and the initial source port via external address and external port. • *restricted-cone*(only UDP): The same as full-cone NAT; for the external host, howev- er, the initial "external" destination host must be used. • *port-restricted-cone*(only UDP): The same as restricted-cone NAT; but only data from the initial destination port are allowed. • *symmetric* (default value) any protocol: In outgoing direction, an external valid source address and an external valid source port are administratively set. In incoming direc- tion, only response packets within the es- tablished connection are permitted.

Fields in the NAT Configuration Specify original traffic menu

Field	Description
Service	Not for **Type of traffic** = *outgoing (Source NAT)* and **NAT**

Field	Description
	method = *full-cone*, *restricted-cone* or *port-restricted-cone*. Select one of the preconfigured services. Possible values: • *User-defined* (default value) • *<Service name>*
Protocol	For certain services only. Not for **Type of traffic** = *outgoing (Source NAT)* and **NAT method** = *full-cone*, *restricted-cone* or *port-restricted-cone*. In this case, UDP is selected automatically. Select a protocol. Depending on the selected service different protocolls are available. Possible values: • *Any* (default value) • *AH* • *Chaos* • *EGP* • *ESP* • *GGP* • *GRE* • *HMP* • *ICMP* • igmp • *IGP* • *IGRP* • *IP* • *IPinIP* • *IPv6* • *IPX in IP* • *ISO-IP*

Field	Description
	• *Kryptolan* • *L2TP* • *OSPF* • *PUP* • *RDP* • *RSVP* • *SKIP* • *TCP* • *TLSP* • *UDP* • *VRRP* • *XNS-IDP*
Source IP Address / Netmask	Enter the source IP address and, if required, the corresponding netmask of the original data packets.
Source Port	Only for **Type of traffic** = *outgoing (Source NAT)*, **NAT method** = *symmetrisch* and **Service** = *User-defined*. Enter the source port of the original data pack- ets. The default setting *All* means that the port is not specified.
Source Port/Range	Not for **Type of traffic** = *outgoing (Source NAT)* Enter the source port or the source port range of the original data packets. The default setting *All* means that the port is not specified.
Destination IP Address / Netmask	Enter the destination IP address and, if required, the corresponding netmask of the original data packets.
Destination Port/Range	Only for **Service** = *User-defined* Enter the destination port or the destination port range of the original data packets. The default setting *All* means that the port is not specified.

In the **NAT Configuration** ->**Substitution values** menu you can define new address and ports, depending on whether the data traffic is incoming or outgoing, to which specific address and ports are translated from the **NAT Configuration** -> **Specify original traffic** menu.

Fields in the NAT Configuration Replacement Values menu

Field	Description
New Destination IP Address/Netmask	Only for **Type of Traffic** = *incoming (Destination NAT)*. Enter the destination IP address and, if required, the corresponding netmask to which the original destination IP address is to be translated.
New Destination Port	Only for **Type of Traffic** = *incoming (Destination NAT)*. Leave the destination port as it appears or enter the destination port to which the original destination port is to be translated. Selecting *Original* leaves the original destina- tion port. If you disable *Original* , an input field appears in which you can enter a new destina- tion port. *Original* is active by default.
Source IP Address / Netmask	Only for **Type of Traffic** = *outgoing (Source NAT)* and **NAT method** = *symmetric*. Enter the source IP address and, if required, the corresponding netmask to which the origi- nal source IP address is to be translated.
New Source Port	Only for **Type of Traffic** = *outgoing (Source NAT)* and **NAT method** = *symmetric*. Leave the source port as it appears or enter a new source port to which the original source port is to be translated. Selecting *Original* leaves the original source port. If you disable *Original*, an input field appears in which you can enter a new source q-port. *Original* is active by default.

14.3 RIP

The entries in the routing table can be defined statically or the routing table can be updated constantly by dynamic exchange of routing information between several devices. This exchange is controlled by a Routing Protocol, e.g. RIP (Routing Information Protocol). By default, about every 30 seconds (this value can be changed in **Update Timer**), a device sends messages to remote networks using information from its own current routing table. The complete routing table is always exchanged in this process. If triggered RIP is used, information is only exchanged if the routing information has changed. In this case, only the changed information is sent.

Observing the information sent by other devices enables new routes and shorter paths for existing routes to be saved in the routing table. As intermediate routes between networks can become unreachable, RIP removes routes that are older than 5 minutes (i.e. routes not verified in the last 300 seconds - **Garbage Collection Timer** + **Route Timeout**). Routes learnt with triggered RIP are not deleted.

Your device supports both version 1 and version 2 of RIP, either individually or together.

14.3.1 RIP Interfaces

In the **Routing** -> **RIP** -> **RIP Interfaces** menu, a list of all RIP interfaces is shown.

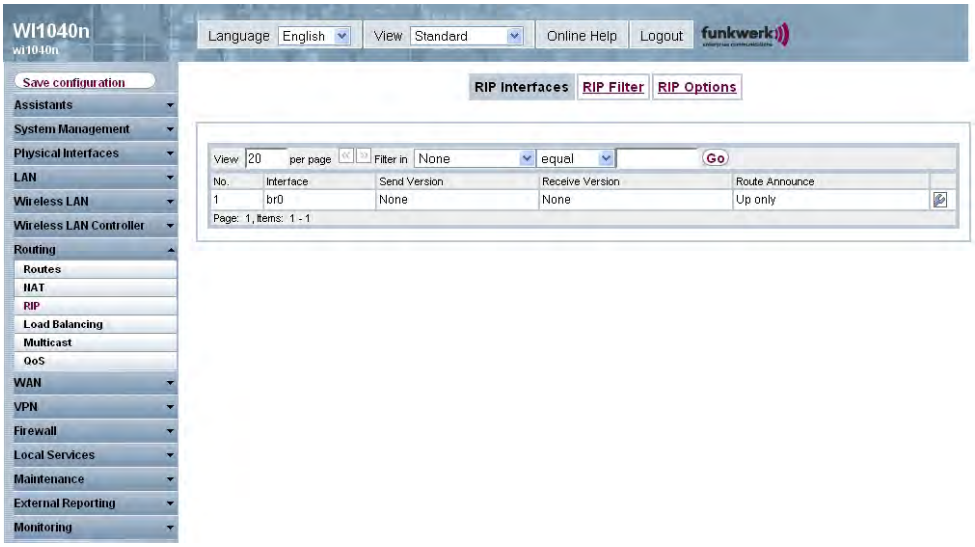


Fig. 94: **Routing** -> **RIP** -> **RIP Interfaces**

14.3.1.1 Edit

For each RIP interface, you can, in the menu, select the options *Send Version*, *Receive Version* and *Route Announce*.

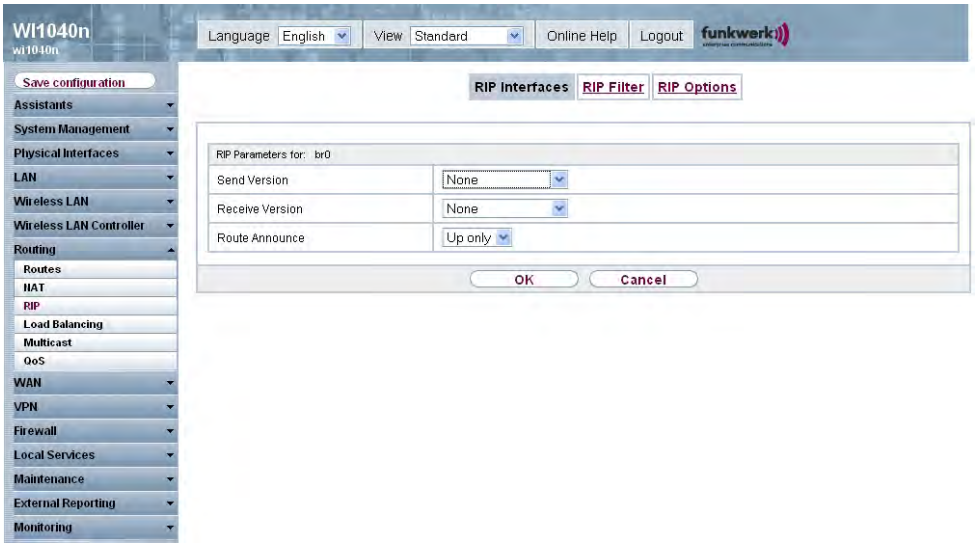


Fig. 95: **Routing -> RIP ->RIP Interfaces->**

The **Routing -> RIP -> RIP Interfaces->** menu consists of the following fields:

Fields in the RIP Parameters for <Interface> menu

Field	Description
Send Version	Decide whether routes are to be propagated via RIP and if so, select the RIP version for sending RIP packets over the interface in send direction. Possible values: • *None* (default value): RIP is not enabled. • *RIP V1*: Enables sending and receiving of version 1 RIP packets. • *RIP V2*: Enables sending and receiving of version 2 RIP packets. • *RIP V1/V2*: Enables sending and receiving of both version 1 and version 2 RIP packets.

Field	Description
	• *RIP V2 Multicast*: For sending RIP V2 messages over the multicast address 224.0.0.9. • *RIP V1 Triggered*: RIP V1 messages are sent, received and processed as per RFC 2091 (triggered RIP). • *RIP V2 Triggered*: RIP V2 messages are sent, received and processed as per RFC 2091 (triggered RIP).
Receive Version	Decide whether routes are to be imported via RIP and if so, select the RIP version for receiving RIP packets over the interface in receive direction. Possible values: • *None* (default value): RIP is not enabled. • *RIP V1*: Enables sending and receiving of version 1 RIP packets. • *RIP V2*: Enables sending and receiving of version 2 RIP packets. • *RIP V1/V2*: Enables sending and receiving of both version 1 and version 2 RIP packets. • *RIP V1 Triggered*: RIP V1 messages are sent, received and processed as per RFC 2091 (triggered RIP). • *RIP V2 Triggered*: RIP V2 messages are sent, received and processed as per RFC 2091 (triggered RIP).
Route Announce	Select this option if you want to set the time at which any activated routing protocols (e.g. RIP) are to propagate the IP routes defined for this interface. Note: This setting does not affect the interface-specific RIP configuration mentioned above. Possible values: • *Up or Dormant* (not for LAN interfaces, interfaces in Bridge mode and interfaces for leased lines): Routes are propagated if the interface status is up or ready. • *Up Only*: Routes are only propagated if the interface status is up. • *Always*: Routes are always propagated independent of operational status.

14.3.2 RIP Filter

In this menu, you can specify exactly which routes are to be exported or imported.

You can use the following strategies for this:

- You explicitly deactivate the import or export of certain routes. The import or export of all other routes that are not listed is still allowed.
- You explicitly activate the import or export of certain routes. In this case, you must also explicitly deactivate the import or export of all other routes. You can do this using a filter for **IP Address** = no entry (this corresponds to the IP address 0.0.0.0) with **Netmask** = no entry (this corresponds to the netmask 0.0.0.0). To make sure this filter is used last, it must be placed at the lowest position.

You configure a filter for a default route with the following values:

- **IP Address** = no entry (this corresponds to the IP address 0.0.0.0) with **Netmask** = 255.255.255.255

In the **Routing** -> **RIP** -> **RIP Filter** menu, a list of all RIP filters is shown.

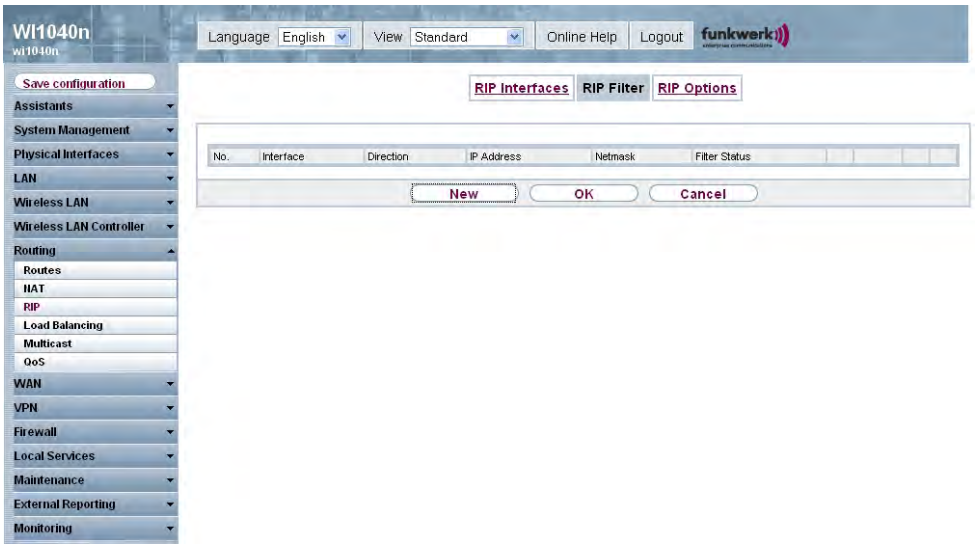


Fig. 96: **Routing** -> **RIP** -> **RIP Filter**

You can use the button to insert another filter above the list entry. The configuration menu for creating a new window opens.

You can use the button to move the list entry. A dialog box opens, in which you can se-

lect the position to which the filter is to be moved.

14.3.2.1 New

Choose the **New** button to set up more RIP filters.

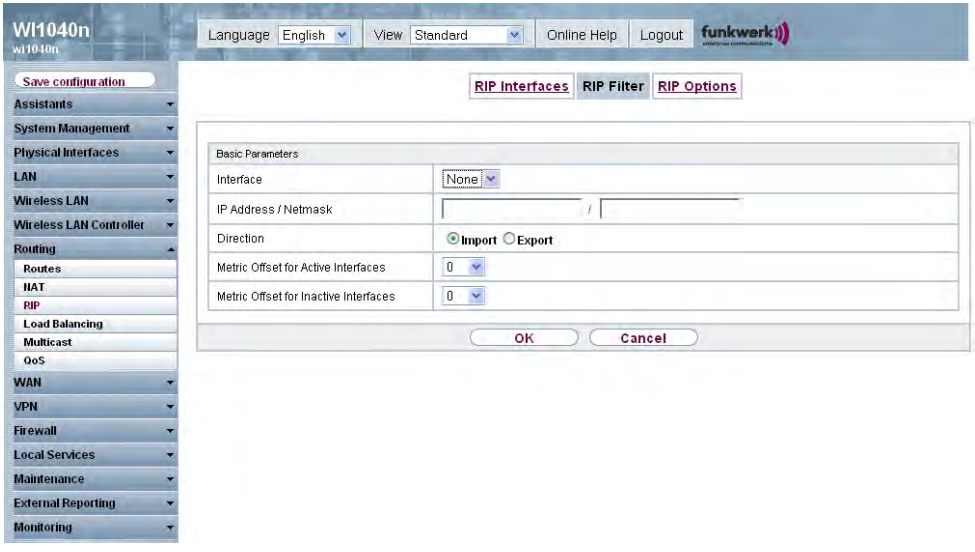


Fig. 97: **Routing** -> **RIP** -> **RIP Filter** -> **New**

The **Routing** -> **RIP** -> **RIP Filter** -> **New** menu consists of the following fields:

Fields in the RIP Filter Basic Parameters menu

Field	Description
Interface	Select the interface to which the rule to be configured applies.
IP Address/Netmask	Enter the IP Address and netmask to which the rule is to be applied. This address can be in the LAN or WAN. The rules for incoming and outgoing RIP packets (import or export) for the same IP address must be separately configured. You can enter individual host addresses or network addresses.
Direction	Select whether the filter applies to the export or import of routes. Possible values: • *Import* (default value) • *Export*

Field	Description
Metric Offset for Active Interfaces	Select the value to be added to the route metric if the status of the interface is "up". During export, the value is added to the exported metric if the interface status is "up". Possible values are `-16` to `16`. The default value is `0`.
Metric Offset for Inactive Interfaces	Select the value to be added to the route metric if the status of the interface is "dormant". During export, the value is added to the exported metric if the interface status is "dormant". Possible values are `-16` to `16`. The default value is `0`.

14.3.3 RIP Options

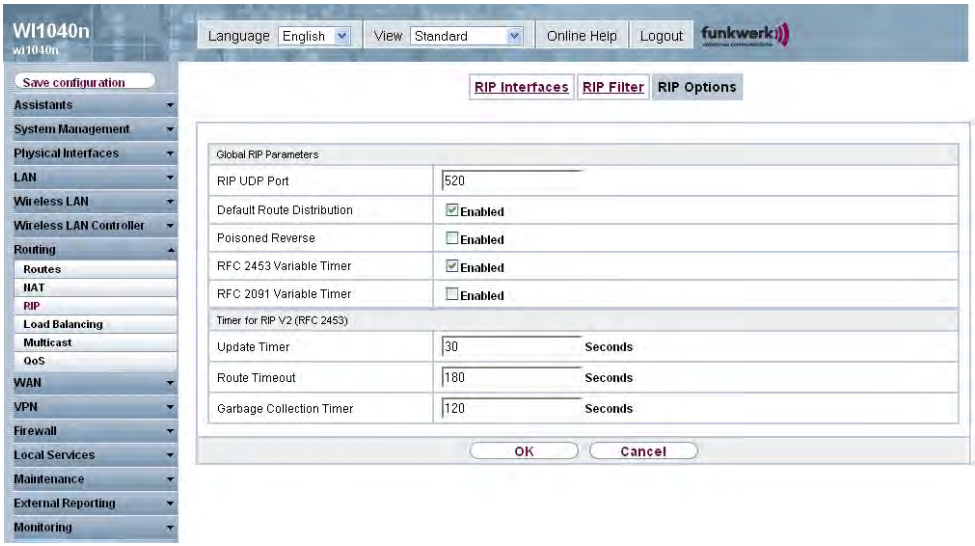


Fig. 98: **Routing** -> **RIP** -> **RIP Options**

The **Routing** -> **RIP** ->**RIP Options** menu consists of the following fields:

Fields in the RIP Options Global RIP Parameters menu

Field	Description
RIP UDP Port	The setting option UDP Port, which is used for sending and re-

Field	Description
	ceiving RIP updates, is only for test purposes. If the setting is changed, this can mean that your device sends and listens at a port that no other devices use. The default value 520 should be retained.
Default Route Distribution	Select whether the default route of your device is to be propagated via RIP updates. The function is activated with *Enabled*. The function is enabled by default.
Poisoned Reverse	Select the procedure for preventing routing loops. With standard RIP, the routes learnt are propagated over all interfaces with RIP SEND activated. With **Poisoned Reverse**, however, your device propagates over the interface over which it learnt the routes, with the metric (Next Hop Count) 16 (=“Network is not reachable“). The function is activated with *Enabled*. The function is disabled by default.
RFC 2453 Variable Timer	For the timers described in RFC 2453, select whether the same values that you can configure in the **Timer for RIP V2 (RFC 2453)** menu. The function is activated with *Enabled*. The function is enabled by default. If you deactivate the function, the times defined in RFC are retained for the timeouts.
RFC 2091 Variable Timer	For the timers described in RFC 2091, select whether the same values that you can configure in the **Timer for Triggered RIP (RFC 2091)** menu. The function is activated with *Enabled*. The function is disabled by default. If the function is not activated, the times defined in RFC are retained for the timeouts.

Fields in the RIP Options Timer for RIP V2 (RFC 2453) menu

Field	Description
Update Timer	Only for **RFC 2453 Variable Timer** = *Enabled* An RIP update is sent on expiry of this period of time. The default value is *30* (seconds).
Route Timeout	Only for **RFC 2453 Variable Timer** = *Enabled* After the last update of a route, the route time is active. After timeout, the route is deactivated and the Garbage Collection Timer is started. The default value is *180* (seconds).
Garbage Collection Timer	Only for **RFC 2453 Variable Timer** = *Enabled* The Garbage Collection Timer is started as soon as the route timeout has expired. After this timeout, the invalid route is deleted from the IPROUTETABLE if no update is carried out for the route. The default value is *120* (seconds).

Fields in the RIP Options Timer for Triggered RIP (RFC 2091) menu

Field	Description
Hold Down Timer	Only for **RFC 2091 Variable Timer** = *Enabled* The hold down timer is activated as soon as your device receives an unreachable route (metric 16). The route may deleted once this period has elapsed. The default value is 120 (seconds).
Retransmission Timer	Only for **RFC 2091 Variable Timer** = *Enabled* After this timeout, update request or update response packets are sent again until an update flush or update acknowledge packet arrives. The default value is 5 (seconds).

14.4 Load Balancing

14.4.1 Load Balancing Groups

The increasing amount of data traffic over the Internet means it is necessary to send data over different interfaces to increase the total bandwidth available. IP load balancing enables the controlled distribution of data traffic within a particular group of interfaces according to the following principles:

- In contrast to Multilink PPP-based solutions, load balancing also functions with accounts with different providers.
- Session-based load balancing is achieved.
- Related (dependent) sessions are always routed over the same interface.
- A decision on distribution is only made for outgoing sessions.

In the **Routing** -> **Load Balancing** -> **Load Balancing Groups** menu a list of all configured load balancing groups is shown.

14.4.1.1 New

Choose the **New** button to set up new groups.

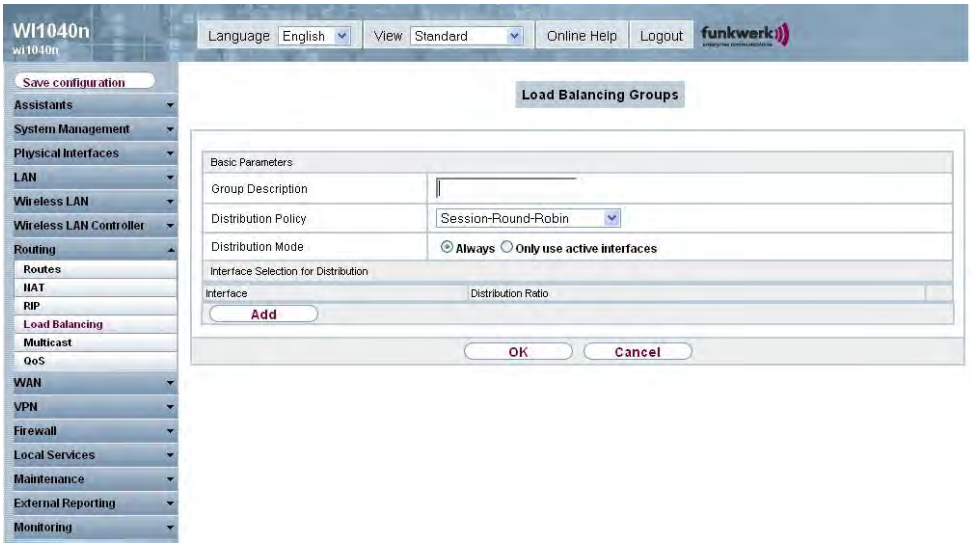


Fig. 99: **Routing** -> **Load Balancing** -> **Load Balancing Groups** -> **New**

The **Routing** -> **Load Balancing** ->**Load Balancing Groups** -> **New** menu consists of the

following fields:

Fields in the Load Balancing Groups Basic Parameters menu

Field	Description
Group Description	Enter the desired description of the interface group.
Distribution Policy	Select the way the data traffic is to be distributed to the interfaces configured for the group. Possible values: • *Session-Round-Robin* (default value): A newly added session is assigned to one of the group interfaces according to the percentage assignment of sessions to the interfaces. The number of sessions is decisive. • *Load-dependent Bandwidth*: A newly added session is assigned to one of the group interfaces according to the share of the total data rate handled by the interfaces. The current data rate based on the data traffic is decisive in both the send and receive direction.
Consider	Only for **Load Balancing Policy** = *Bandwidth, load-dependent* Choose the direction in which the current data rate is to be considered. Options: • *Download*: Only the data rate in the receive direction is considered. • *Upload*: Only the data rate in the send direction is considered. The *Download* and *Upload* are deactivated by default.
Distribution Mode	Select the state the interfaces in the group may have if they are to be included in load balancing. Possible values: • *Always*(default value): Also includes idle interfaces. • *Only use active interfaces*: Only interfaces in the up state are included.

In the **Interface Selection for Load Balancing** area, you add and configure interfaces that match the current group context. You can also delete interfaces.

Use **Add** to create entries.

Fields in the Load Balancing Groups Interface Selection for Distribution menu

Field	Description
Interface	Select the interfaces that are to belong to the group from the available interfaces.
Distribution Ratio	Enter the percentage of the data traffic to be assigned to an interface. The meaning differs according to the **Distribution Policy** used: • Based on the number of sessions to be distributed for *Session-Round-Robin*. • For *Bandwidth Load Dependent* the data rate is the decisive factor.

14.5 Multicast

What is multicasting?

Many new communication technologies are based on communication from one sender to several recipients. Therefore, modern telecommunication systems such as voice over IP or video and audio streaming (e.g. IPTV or Webradio) focus on reducing data traffic, e.g. by offering TriplePlay (voice, video, data). Multicast is a cost-effective solution for effective use of bandwidth because the sender of the data packet, which can be received by several recipients, only needs to send the packet once. The packet is sent to a virtual address defined as a multicast group. Interested recipients log in to these groups.

Other areas of use

One classic area in which multicast is used is for conferences (audio/video) with several recipients. The most well-known are probably the MBone Multimedia Audio Tool (VAT), Video Conferencing Tool (VIC) and Whiteboard (WB). VAT can be used to hold audio conferences. All subscribers are displayed in a window and the speaker(s) are indicated by a black box. Other areas of use are of particular interest to companies. Here, multicasting makes it possible to synchronise the databases of several servers, which is valuable for multinationals or even companies with just a few locations.

Address range for multicast

For, IPv4 the IP addresses 224.0.0.0 to 239.255.255.255 (224.0.0.0/4) are reserved for multicast in the class D network. An IP address from this range represents a multicast group to which several recipients can log in. The multicast router then forwards the required packets to all subnets with logged in recipients.

Multicast basics

Multicast is connectionless, which means that any trouble-shooting or flow control needs to be guaranteed at application level.

At transport level, UDP is used almost exclusively, as, in contrast to TCP, it is not based on a point-to-point connection.

At IP level, the main difference is therefore that the destination address does not address a dedicated host, but rather a group, i.e. during the routing of multicast packets, the decisive factor is whether a recipient is in a logged-in subnet.

In the local network, all hosts are required to accept all multicast packets. For Ethernet or FDD, this is based on MAC mapping, where the group address is encoded into the destination MAC address. For routing between several networks, the routers first need to make themselves known to all potential recipients in the subnet. This is achieved by means of Membership Management protocols such as IGMP for IPv4 and MLP for IPv6.

Membership Management protocol

In IPv4, IGMP (Internet Group Management Protocol) is a protocol that hosts can use to provide the router with multicast membership information. IP addresses of the class D address range are used for addressing. An IP address in this class represents a group. A sender (e.g. Internet radio) sends data to this group. The addresses (IP) of the various senders within a group are called the source (addresses). Several senders (with different IP addresses) can therefore transmit to the same multicast group, leading to a 1-to-n relationship between groups and source addresses. This information is forwarded to the router by means of reports. In the case of incoming multicast data traffic, a router can use this information to decide whether a host in its subnet wants to receive it. Your device supports the current version IGMP V3, which is upwardly compatible, which means that both V3 and V1/V2 hosts can be managed.

Your device supports the following multicast mechanisms:

- Forwarding: This relates to static forwarding, i.e. incoming data traffic for a group is passed in all cases. This is a useful option if multicast data traffic is to be permanently

passed.

- IGMP: IGMP is used to gather information about the potential recipients in a subnet. In the case of a hop, incoming multicast data traffic can thus be selected.

Tip

With multicast, the focus is on excluding data traffic from unwanted multicast groups. Note that if forwarding is combined with IGMP, the packets can be forwarded to the groups specified in the forwarding request.

14.5.1 Forwarding

In this menu, you specify which multicast groups are always passed between the interfaces of your device.

14.5.1.1 New

Choose the **New** button to create forwarding rules for new multicast groups.

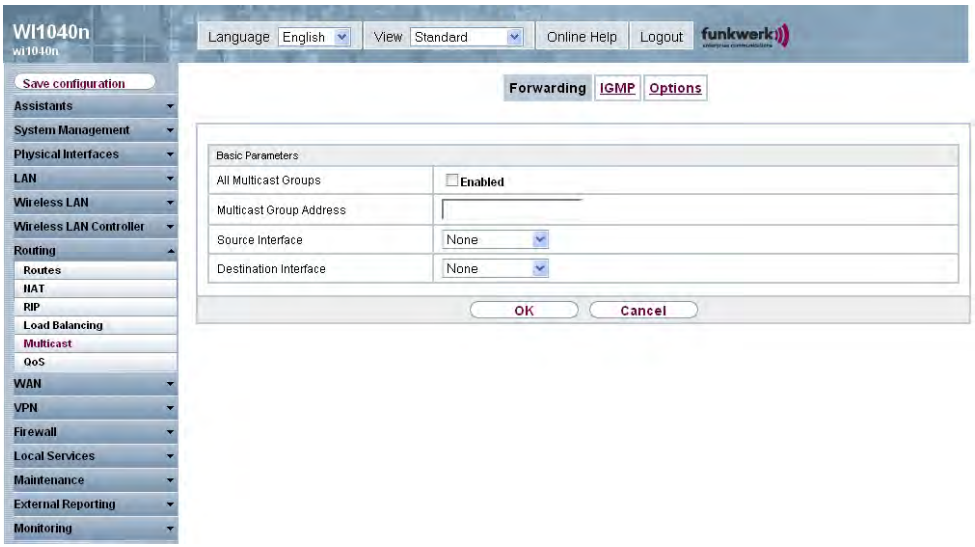


Fig. 100: **Routing** -> **Multicast** -> **Forwarding** -> **/New**

The **Routing** -> **Multicast** -> **Forward** -> **/New** menu consists of the following fields:

Fields in the Forwarding Basic Parameters menu

Field	Description
All Multicast Groups	Select whether all multicast groups, i.e. the complete multicast address range 224.0.0.0/4, are to be forwarded from the defined **Source Interface** to the defined **Destination Interface** To do this, check **Enabled** Disable the option if you only want to forward one defined multicast group to a particular interface. The option is deactivated by default.
Multicast Group Address	Only for **All Multicast-Groups** = *disabled* Enter here the address of the multicast group you want to forward from a defined **Source Interface** to a defined **Destination Interface**
Source Interface	Select the interface on your device to which the selected multicast group is sent.
Destination Interface	Select the interface on your device to which the selected multicast group is to be forwarded.

14.5.2 IGMP

IGMP (Internet Group Management Protocol, see RFC 3376) is used to signal the information about group (membership) in a subnet. As a result, only the packets explicitly wanted by a host enter the subnet.

Special mechanisms ensure that the requirements of the individual clients are taken into consideration. At the moment there are three versions of IGMP (V1 - V3); most current systems use V3, and less often V2.

Two packet types play a central role in IGMP: queries and reports.

Queries are only transmitted from a router. If several IGMP routers exist in a network, the router with the lowest IP address is the "querier". We differentiate here between a general query (sent to 224.0.0.1), a group-specific query (sent to a group address) and the group-and-source-specific query (sent to a specific group address). Reports are only sent by hosts to respond to queries.

In this menu, you configure the interfaces on which IGMP is to be enabled.

14.5.2.1 New

Choose the **New** button to configure IGMP on other interfaces.

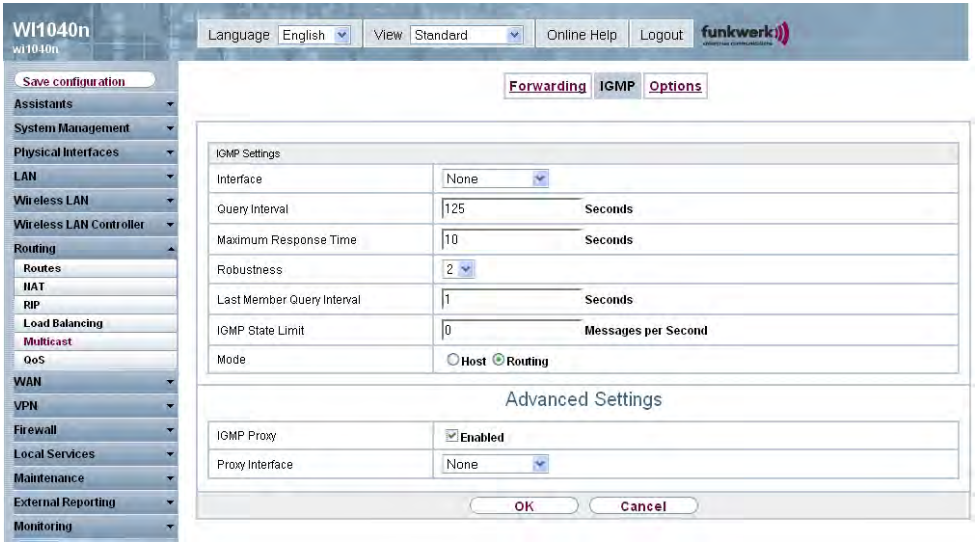


Fig. 101: **Routing** -> **Multicast** -> **IGMP** -> **/New**

The **Routing** -> **Multicast** -> **IGMP** -> **/New** menu consists of the following fields:

Fields in the IGMP IGMP Settings menu

Field	Description
Interface	Select the interface on which IGMP is to be enabled, i.e. queries are sent and responses are accepted.
Query Interval	Enter the interval in seconds in which IGMP queries are to be sent. Possible values are `0` to `600`. The default value is `125`.
Maximum Response Time	For the sending of queries, enter the time interval in seconds within which hosts must respond. The hosts randomly select a time delay from this interval before sending the response. This spreads the load in networks with several hosts, improving performance.

Field	Description
	Possible values are *0* to *100*. The default value is *100*.
Robustness	Select the multiplier for controlling the timer values. A higher value can e.g. compensate for packet loss in a network susceptible to loss. If the value is too high, however, the time between logging off and stopping of the data traffic can be increased (leave latency). Possible values are *2* to *8*. The default value is *2*.
Last Member Query Interval	Define the time after a query for which the router waits for an answer. If you shorten the interval, it will be more quickly detected that the last member has left a group so that no more packets for this group should be forwarded to this interface. Possible values are *0* to *255*. The default value is *10*.
IGMP State Limit	Limit the number of reports/queries per second for the selected interface.
Mode	Specify whether the interface defined here only works in host mode or in both host mode and routing mode. Possible values: • *Host and Routing* (default value): The interface is operated in routing mode and in host mode. • *Host only*: The interface is only operated in host mode.

IGMP Proxy

IGMP Proxy enables you to simulate several locally connected interfaces as a subnet to an adjacent router. Queries coming in to the IGMP Proxy interface are forwarded to the local subnets. Local reports are forwarded on the IPGM Proxy interface.

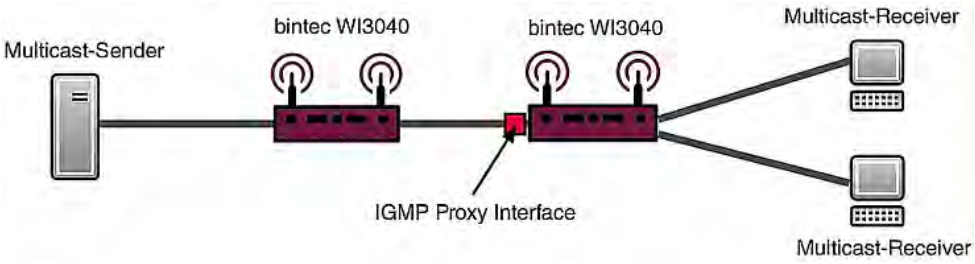


Fig. 102: IGMP Proxy

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
IGMP Proxy	Select whether your device is to forward the hosts' IGMP messages in the subnet via its defined **Proxy Interface**.
Proxy Interface	Select the interface on your device via which queries are to be received and collected.

14.5.3 Options

In this menu, you can enable and disable IGMP on your system. You can also define whether IGMP is to be used in compatibility mode or only IGMP V3 hosts are to be accepted.

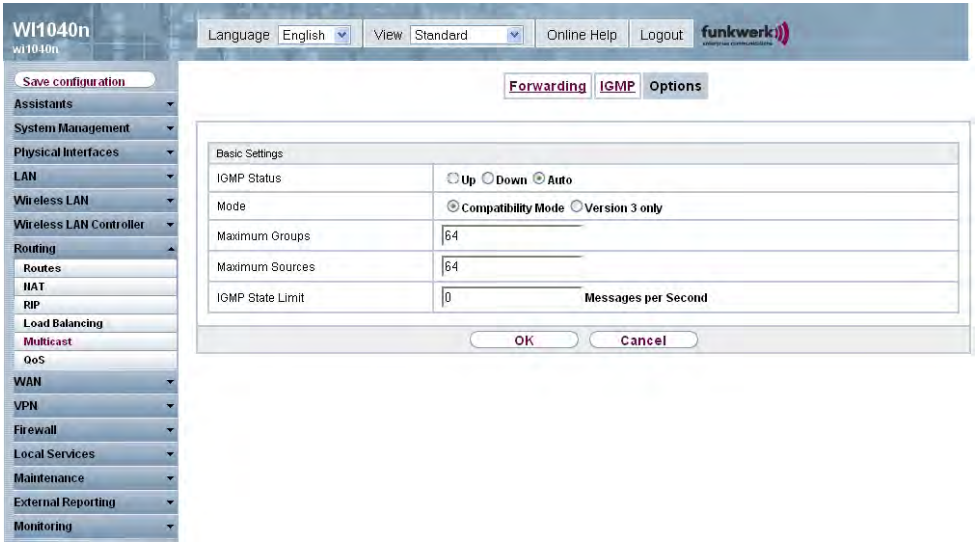


Fig. 103: **Routing** -> **Multicast** -> **Options**

The **Routing** -> **Multicast** -> **Options** menu consists of the following fields:

Fields in the Options Basic Settings menu

Field	Description
IGMP Status	Select the IGMP status. Possible values: • *auto* (default value) Multicast is activated automatically for hosts if the hosts open applications that use multicast. • *Active*: Multicast is always on. • *Down* : Multicast is always off.
Mode	Only for **IGMP Status** = *Active* or *Auto* Select Multicast Mode. Possible values: • *Compatibility Mode* (default value): The router uses IGMP version 3. If it notices a lower version in the network, it uses the lowest version it could detect. • *Version 3 only*: Only IGMP version 3 is used.
Maximum Groups	Enter the maximum number of groups to be permitted, both in-

Field	Description
	ternally and in reports.
Maximum Sources	Enter the maximum number of sources that are specified in version 3 reports and the maximum number of internally managed sources per group.
IGMP State Limit	Enter the maximum permitted total number of incoming queries and messages per second. The default value is `0`, i.e. the number of IGMP status messages is not limited.

14.6 QoS

QoS (Quality of Service) makes it possible to distribute the available bandwidths effectively and intelligently. Certain applications can be given preference and bandwidth reserved for them. This is an advantage, especially for time-critical applications such as VoIP.

The QoS configuration consists of three parts:

- Creating IP filters
- Classifying data
- Prioritising data.

14.6.1 QoS Filter

IP filters are configured in the **Routing** -> **QoS** -> **QoS Filter** menu.

14.6.1.1 New

Choose the **New** button to define more IP filters.

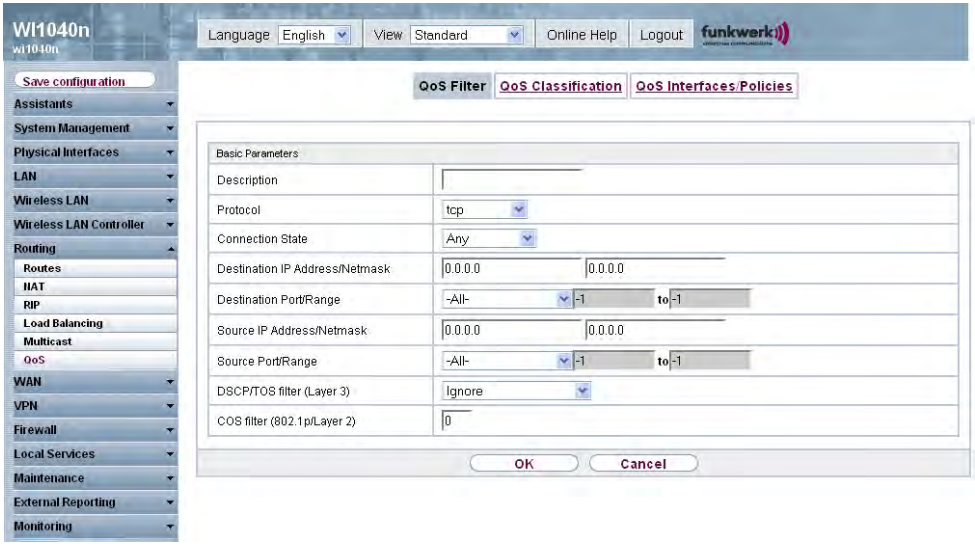


Fig. 104: **Routing** -> **QoS** -> **QoS Filter** -> **New**

The **Routing**-> **QoS** -> **QoS Filter** -> **New** menu consists of the following fields:

Fields in the QoS Filter Basic Parameters menu

Field	Description
Description	Enter the name of the filter.
Protocol	Select a protocol. Possible values: *l2tp*, *ah*, *Chaos*, *dont-verify*, *egp*, *esp*, *ggp*, *gre*, *hmp*, *icmp*, *igmp*, *IGP*, *igrp*, *IP*, *ipip*, *ipv6*, *IPX in IP*, *ISO-IP*, *Kryptolan*, *ospf*, *pim*, *pup*, *rdp*, *rsvp*, *SKIP*, *tcp*, *TLSP*, *udp*, *VRRP*, *xns-idp*. The *Do not verify* option (default value) matches any protocol.
Type	Only if **Protocol** = *icmp* Select the type. Possible values: *Any*, *Echo reply*, *Destination unreachable*, *Source quench*, *Redirect*, *Echo*, *Time expired*, *Timestamp*, *Timestamp reply*. See RFC 792.

Field	Description
	The default value is *Any* .
Connection State	If **Protocol** = *tcp*, you can define a filter that takes the status of the TCP connections into account. Possible values: • *Established*: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter. • *Any* (default value): All TCP packets match the filter.
Destination IP Address / Netmask	Enter the destination IP address of the data packets and the corresponding netmask.
Destination Port/Range	Only if **Protocol** = *tcp* or *udp* Enter a destination port number or a range of destination port numbers. Possible values: • *All* (default value): The destination port is not specified. • *Specify port* : Enter a destination port. • *Specify port range* : Enter a destination port range.
Source IP Address / Netmask	Enter the source IP address of the data packets and the corresponding netmask.
Source Port/Range	Only if **Protocol** = *tcp* or *udp* Enter a source port number or a range of source port numbers. Possible values: • *All* (default value): The destination port is not specified. • *Specify port* : Enter a destination port. • *Specify port range* : Enter a destination port range.
DSCP/TOS filter (Layer 3)	Specify how the priority of the IP packets is signalled. Possible values: • *Ignore* (default value): No priority signalling is used. • *DSCP Binary Value*: Differentiated Services Code Point is

Field	Description
	used to signal the priority of IP packets (indicated in binary format; currently not implemented). • *DSCP Decimal Value*: Differentiated Services Code Point is used to signal the priority of IP packets (indicated in decimal format; possible values *0* to *63*; currently not implemented). • *TOS Binary Value*: Type of Service is used to signal the priority of IP packets (indicated in binary format). • *TOS Decimal Value*: Type of Service is used to signal the priority of IP packets (indicated in decimal format; possible values *0* to *255*).
COS filter (802.1p/Layer 2)	Enter the service class of the IP packets (Class of service, CoS). Possible values: *0* and *7*. The default value is *0*.

14.6.2 QoS Classification

The data traffic is classified in the **Routing** -> **QoS** -> **QoS Classification** menu, i.e. the data traffic is associated using class IDs of various classes. To do this, create class plans for classifying IP packets based on pre-defined IP filters. Each class plan is associated to at least one interface via its first filter.

14.6.2.1 New

Choose the **New** button to set up other data classes.

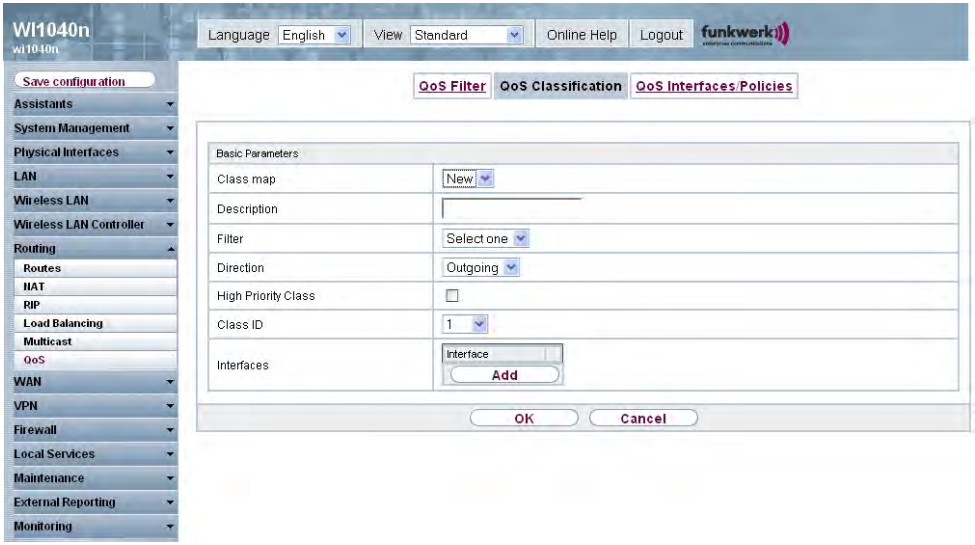


Fig. 105: **Routing** -> **QoS** -> **QoS Classification** -> **New**

The **Routing** -> **QoS** -> **QoS Classification** -> **New** menu consists of the following fields:

Fields in the QoS Classification Basic Parameters menu

Field	Description
Class map	Choose the class plan you want to create or edit. Possible values: • *New* (default value): You can create a new class plan with this setting. • *<Name of class plan>*: Shows a class plan that has already been created, which you can select and edit.
Description	Only if **Class map** = *New*. Enter the name of the class plan.
Filter	Select an IP filter. If the class plan is new, select the filter to be set at the first point of the class plan. If the class plan already exists, select the filter to be attached to the class plan. To select a filter, at least one filter must be configured in the

Field	Description
	Routing -> **QoS** -> **QoS Filter** menu.
Direction	Select the direction of the data packets to be classified. Possible values: • *Incoming* : Incoming data packets are to be classified. • *Outgoing* (default value): Outgoing data packets are to be classified. • *Both* : Incoming and outgoing data packets are to be classified.
High Priority Class	Enable or disable the high priority class. If the high priority class is active, the data packets are associated with the class with the highest priority and priority 0 is set automatically. The function is activated with *Enabled*. The function is disabled by default.
Class ID	Only if **High Priority Class** is inactive. Choose a number which assigns the data packets to a class. Note: The class ID is a label to assign data packets to specific classes. (The class ID defines the priority.) Possible values are whole numbers between *1* and *254*.
Interfaces	Only if **Class map** = *New*. When creating a new class plan, select the interfaces to which you want to link the class plan. A class plan can be assigned to multiple interfaces.

14.6.3 QoS Interfaces/Policies

You can define the priority in the **Routing** -> **QoS** -> **QoS Interfaces/Policies** menu.

Note

Data can only be prioritized in the outgoing direction.

Packets in the high-priority class always take priority over data with class IDs 1... 254.

It is possible to assign or guarantee each queue and thus each data class a certain part of the total bandwidth of the interface. In addition, you can optimise the transmission of voice data (real time data).

Depending on the respective interface, a queue is created automatically for each class, but only for data traffic classified as outgoing and for data traffic classified in both directions. A priority is assigned to these automatic queues. The value of the priority is equal to the value of the class ID. You can change the default priority of a queue. If you add new queues, you can also use classes in other class plans via the class IDs.

14.6.3.1 New

Choose the **New** button to set up other priorities.

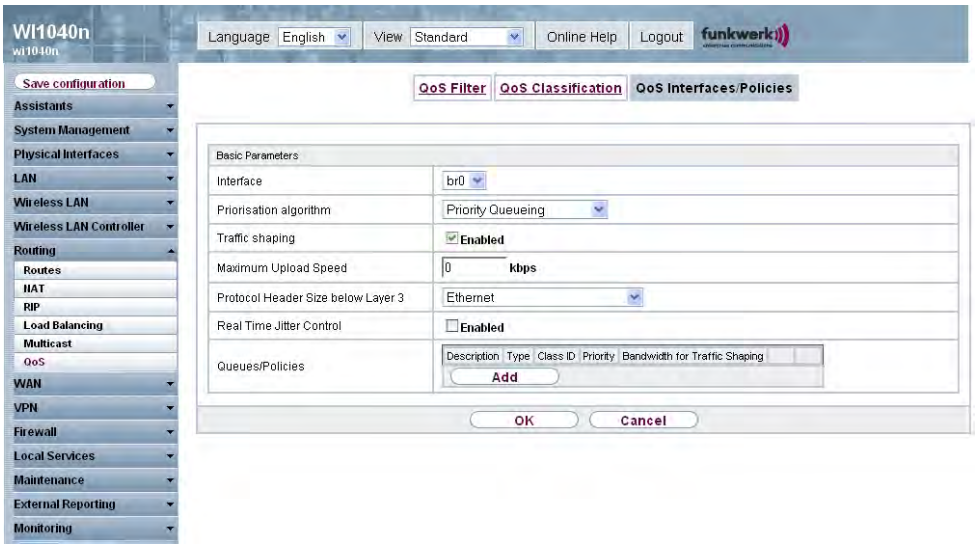


Fig. 106: **Routing** -> **QoS** -> **QoS Interfaces/Policies** -> **New**

The **Routing**-> **QoS** -> **QoS Interfaces/Policies** -> **New** menu consists of the following fields:

Fields in the QoS Interfaces/Policies Basic Parameters menu

Field	Description
Interface	Select the interface for which QoS is to be configured.

Field	Description
Priorisation algorithm	Select the algorithm according to which the queues are to be processed. This activates and deactivates QoS on the selected interface. Possible values: • *Priority Queueing*(default value): QoS is activated on the interface. The available bandwidth is distributed strictly according to the queue priority. • *Weighted Round Robin*: QoS is activated on the interface. The available bandwidth is distributed according to the weighting (weight) of the queue. Exception: High-priority packets are always handled with priority. • *Weighted Fair Queueing*: QoS is activated on the interface. The available bandwidth is distributed as “fairly” as possible among the (automatically detected) traffic flows in a queue. Exception: High-priority packets are always handled with priority. • *Disabled* : QoS is deactivated on the interface. The existing configuration is not deleted, but can be activated again if required.
Traffic shaping	Activate or deactivate data rate limiting in the send direction. The function is activated with *Enabled*. The function is disabled by default.
Maximum Upload Speed	Only enabled for **Traffic shaping** . Enter a maximum data rate for the interfaces in the send direction in kbits. Possible values are *1* to *1000000*. The default value is *0*, i.e. no limits are set, the queue can occupy the maximum bandwidth.
Protocol Header Size below Layer 3	Choose the interface type to include the size of the respective overheads of a datagram when calculating the bandwidth. Possible values: • *Custom* (value in Byte; possible values are *0* to *100*.)

Field	Description
	• *Ethernet* (default value) • *Ethernet and VLAN* • *PPPoE* • *PPPoE and VLAN* • *IPSec over Ethernet* • *IPSec over Ethernet and VLAN* • *IPSec via PPP over Ethernet* • *IPSec via PPPoE and VLAN*
Real Time Jitter Control	Only enabled for **Transmit Shaping**. Real Time Jitter Control optimises latency when forwarding real time datagrams. The function ensures that large data packets are fragmented according to the available upload bandwidth. Real Time Jitter Control is useful for small upload bandwidths (< 800 kbps). Activate or deactivate Real Time Jitter Control. The function is activated with *Enabled*. The function is disabled by default.
Control Mode	Only if **Real Time Jitter Control** = Enabled. Select the mode for optimising voice transmission. Possible values: • *All RTP Streams*: All RTP streams are optimised. The function activates the RTP stream detection mechanism for the automatic detection of RTP streams. In this mode, the Real Time Jitter Control is activated as soon as an RTP stream has been detected. • *Inactive* : Voice data transmission is not optimised. • *Controlled RTP Streams only*(default value): This mode is used if either the VoIP Application Layer Gateway (ALG) or the VoIP Media Gateway (MGW) is active. Real Time Jitter Control is activated by the control instances ALG or MGW. • *Always*: Real Time Jitter Control is always active, even if no

Field	Description
	real time data is routed.
Queues/Policies	Configure the desired QoS queues. For each class created from the class plan, which is associated with the selected interface, a queue is generated automatically and displayed here (only for outgoing classified data traffic and for data traffic classified in both directions). Add a new entry with **Add**. The **Edit Queues/Policies** menu opens.

The **Edit Queues/Policies** menu consists of the following fields:

Fields in the Edit Queues/Policies menu

Field	Description
Description	Enter the name of the queue/policy.
Outgoing Interface	Shows the interface for which the QoS Queues are being configured.
Priorisation queue	Select the queue priority type. Possible values: • *Class Based* (default value): Queue for data classified as “normal”. • *High Priority*: Queue for data classified as “high priority”. • *Default*: Queue for data that has not been classified or data of a class for which no specific queue has been configured.
Class ID	Only if **Priority Queue** = *Class based*. Select the QoS packet class to which this queue is to apply. To do this, at least one class ID must be given in the **Routing** -> **QoS** -> **QoS Classification** menu.
Priority	Only if **Priority Queue** = *Class based*. Choose the priority of the queue. Possible values are *1* to *254*. The default value is *1*.

Field	Description
Weight	Only if **Priorisation algorithm** = *Weighted Round Robin* or *Weighted Fair Queueing* Choose the weight of the queue. Possible values are *1* to *254*. The default value is *1*.
RTT Mode (Realtime Traffic Mode)	Active or deactivate the real time transmission of the data. The function is activated with *Enabled*. The function is disabled by default. RTT Mode should be activated for QoS classes in which real time data has priority. This mode improves latency when forwarding real time datagrams. It is possible to configure multiple queues when RTT Mode is enabled. Queues with enabled RTT mode must always have a higher priority than queues with disabled RTT Mode.
Traffic Shaping	Activate or deactivate data rate (=Traffic Shaping) limiting in the send direction. The data rate limit applies to the selected queue. (This is not the limit that can be defined on the interface.) The function is activated with *Enabled*. The function is disabled by default.
Maximum Upload Speed	Only for **Traffic Shaping** = Enabled. Enter a maximum data rate for the queue in kbits. Possible values are *0* to *1000000*. The default value is *0*.
Overbooking allowed	Only for **Traffic Shaping** = Enabled. Enable or disable the function. The function controls the bandwidth limit. If **Overbooking allows** is activated, the bandwidth limit set for this queue can be exceeded, as long as free bandwidth exists

Field	Description
	on the interface. If **Overbooking allowed** is deactivated, the queue can never occupy bandwidth beyond the bandwidth limit that has been set. The function is activated with *Enabled*. The function is disabled by default.
Burst size	Only for **Traffic Shaping** = Enabled. Enter the maximum number of bytes that may still be transmitted temporarily when the data rate permitted for this queue has been reached. Possible values are *0* to *64000*. The default value is *0*.

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Dropping algorithm	Choose the procedure for rejecting packets in the QoS Queue, if the maximum size of the queue is exceeded. Possible values: • *Tail Drop* (default value): The newest packet received is dropped. • *Head Drop*: The oldest packet in the queue is dropped. • *Random Drop*: A randomly selected packet is dropped from the queue.
Min. queue size	Enter the minimum size of the queue in bytes. Possible values are *0* to *16384*. The default value is *0*.
Max. queue size	Enter the maximum size of the queue in bytes. Possible values are *0* to *16384*. The default value is *16384*.

Chapter 15 WAN

This menu offers various options for configuring accesses or connections from your LAN to the WAN. You can also optimise voice transmission here for telephone calls over the Internet.

15.1 Internet + Dialup

In this menu, you can set up Internet access or dialup connections.

To enable your device to set up connections to networks or hosts outside your LAN, you must configure the partners you want to connect to on your device. This applies to outgoing connections (your device dials its WAN partner) and incoming connections (a remote partner dials the number of your device).

If you want to set up Internet access, you must set up a connection to your Internet Service Provider (ISP). For broadband Internet access, your device provides the PPP-over-Ethernet (PPPoE) and PPP-over-PPTP protocols.

Note

Note your provider's instructions.

All the entered connections are displayed in the corresponding list, which contains the **Description**, the **User Name**, the **Authentication** and the current **Status**.

The **Status** field can take the following values:

Possible values for Status:

Field	Description
	connected
	not connected (dialup connection); connection setup possible
	not connected (e.g. because of an error during setup of an outgoing connection, a renewed attempt is only possible after a specified number of seconds)
	administratively set to down (deactivated); connection setup not possible for leased lines:

Default Route

With a default route, all data is automatically forwarded to one connection if no other suitable route is available. Access to the Internet should always be set up as the default route to the Internet Service Provider (ISP). Further information on possible route types can be found under **Routing** -> **Routes**.

Activating NAT

With Network Address Translation (NAT), you conceal your whole network to the outside world behind one IP address. You should certainly do this for your connection to the Internet Service Provider (ISP).

Only outgoing sessions are allowed initially if NAT is activated. To allow certain connections from outside to hosts within the LAN, these must be explicitly defined and admitted.

Connection Idle Timeout

The connection idle timeout is determined in order to clear the connection automatically if it is not being used, i.e. if data is no longer being sent, to help you save costs.

Block after Connection Failure

You use this function to set up a waiting time for outgoing connection attempts after which your device's connection attempt is regarded as having failed.

Authentication

When a call is received on ISDN connections, the calling party number is always sent over the ISDN D-channel. This number enables your device to identify the caller (CLID), provided the caller is entered on your device. After identification with CLID, your device can additionally carry out PPP authentication with the connection partner before it accepts the call.

Your device needs the necessary data for this, which you should enter here, for all PPP connections. Establish the type of authentication process that should be performed, then enter a common password and two codes. You get this information, for example, from your Internet Service Provider (ISP) or the system administrator at your head office. If the data you entered on your device is the same as the caller's data, the call is accepted. The call is rejected if the data is not the same.

15.1.1 PPPoE

In the **WAN** -> **Internet + Dialup** -> **PPPoE** menu, a list of all PPPoE interfaces is shown.

PPP over Ethernet (PPPoE) is the use of the Point-to-Point Protocol (PPP) network protocol over an Ethernet connection. Today, PPPoE is used for ADSL connections in Germany. In Austria, the Point To Point Tunnelling Protocol (PPTP) was originally used for ADSL access. However, PPPoE is now offered here too by some providers.

15.1.1.1 New

Choose the **New** button to set up new PPPoE interfaces.

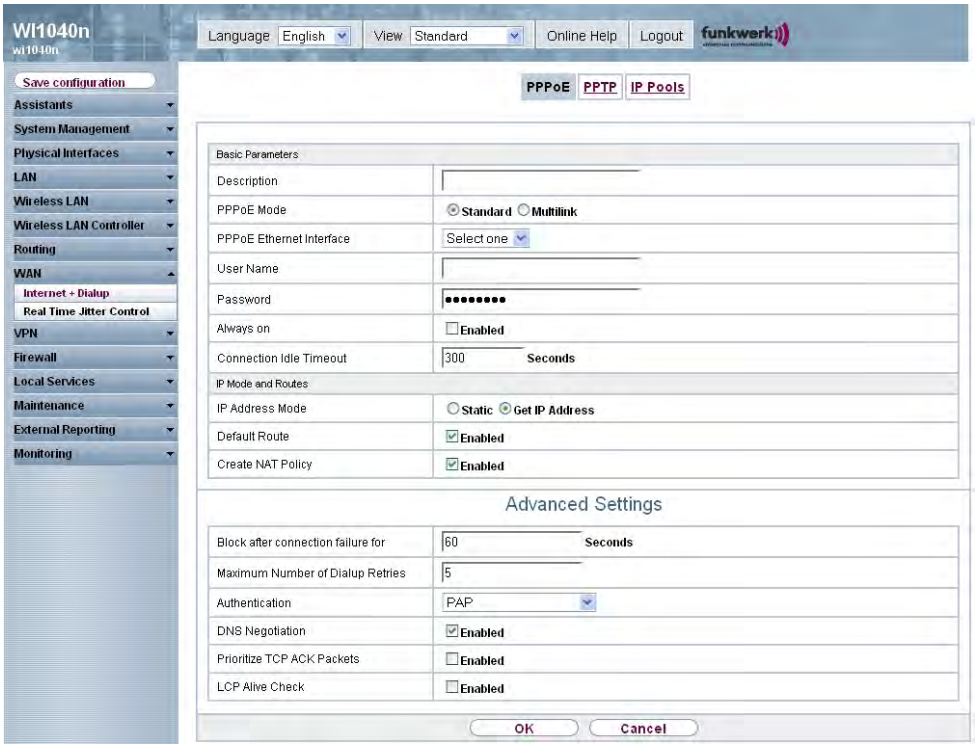


Fig. 107: **WAN** -> **Internet + Dialup** -> **PPPoE** -> **New**

The **WAN** -> **Internet + Dialup** -> **PPPoE** -> **New** menu consists of the following fields:

Fields in the PPPoE Basic Parameters menu

Field	Description
Description	Enter a name to uniquely identify the PPPoE partner. The first character in this field must not be a number and no special characters or umlauts must be used.
PPPoE Mode	Select whether you want to use a standard Internet connection over PPPoE (*Standard*) or your Internet access is to be set up over several interfaces (*Multilink*). If you choose *Multilink*, you can connect several DSL connections from a provider over PPP as a static bundle in order to obtain more bandwidth. Each of these DSL connections should use a separate Ethernet connection for this. At the moment, many providers are still in the process of preparing the PPPoE Multilink function. For PPPoE Multilink, we recommend using your device's Ethernet switch in Split-Port mode and to use a separate Ethernet interface e.g. *en1-1*, *en1-2* for each PPPoE connection. If you also want to use an external modem for PPPoE Multilink, you must run your device's Ethernet switch in Split-Port mode.
PPPoE Ethernet Interface	Only if **PPPoE Mode** = *Standard* Select the Ethernet interface specified for a standard PPPoE connection. If you want to use an external DSL modem, select the Ethernet port to which the modem is connected. When using the internal DSL modem, select here the EthoA interface configured in **Physical Interfaces**-> **ATM**-> **Profiles**-> **New**. The default value is *Not specified*.
PPPoE Interfaces for Multilink	Only if **PPPoE Mode** = *Multilink* Select the interfaces you want to use for your Internet connection. Click the **Add** button to create new entries.
User Name	Enter the user name.
Password	Enter the password.
Always on	Select whether the interface should always be activated.

Field	Description
	The function is activated with *Enabled*. The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the short hold. The default value is *300*. Example: *10* for FTP transmission, *20* for LAN-to-LAN transmission, *90* for Internet connections.

Fields in the PPPoE IP Mode and Routes menu

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *Get IP Address* (default value): Your device is dynamically assigned an IP address. • *Static*: You enter a static IP address.
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is activated with *Enabled*. The function is enabled by default.
Create NAT Policy	Specify whether Network Address Translation (NAT) is to be activated. The function is activated with *Enabled*.

Field	Description
	The function is enabled by default.
Local IP Address	Only if **IP Address Mode** = *Static* Enter the static IP address of the connection partner.
Route Entries	Only if **IP Address Mode** = *Static* Define other routing entries for this connection partner. Add a new entry with **Add**. • *Remote IP Address*: IP address of the destination host or network. • *Netmask*: Netmask of **Remote IP Address**. If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (possible values *0*... *15*). The default value is *1*.

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *60*.
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked. Possible values are *0* to *100*. The default value is *5*.
Authentication	Select the authentication protocol for this connection partner. Select the authentication specified by your provider. Possible values: • *PAP* (default value) Only run *PAP* (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Only run *CHAP* (PPP Challenge Handshake Authentication Protocol as per RFC 1994); the password is transferred

Field	Description
	encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP* : Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.) • *MS-CHAPv2*: Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
DNS Negotiation	Select whether your device receives IP addresses for **Primary DNS Server** and **Secondary DNS Server** from the connection partner or sends these to the connection partner. The function is activated with *Enabled*. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is activated with *Enabled*. The function is disabled by default.
LCP Alive Check	Check whether the reachability of the remote terminal is to be checked by sending LCP echo requests or replies. This makes it possible to switch to a backup connection more quickly in the event of line faults. The function is activated with *Enabled*. The function is disabled by default.

15.1.2 PPTP

In the **WAN** -> **Internet + Dialup** -> **PPTP** menu, a list of all PPTP interfaces is shown.

In this menu, you configure an Internet connection that uses the Point Tunnelling Protocol (PPTP) to set up a connection, e.g. required in Austria.

15.1.2.1 New

Choose the **New** button to set up new PPTP interfaces.

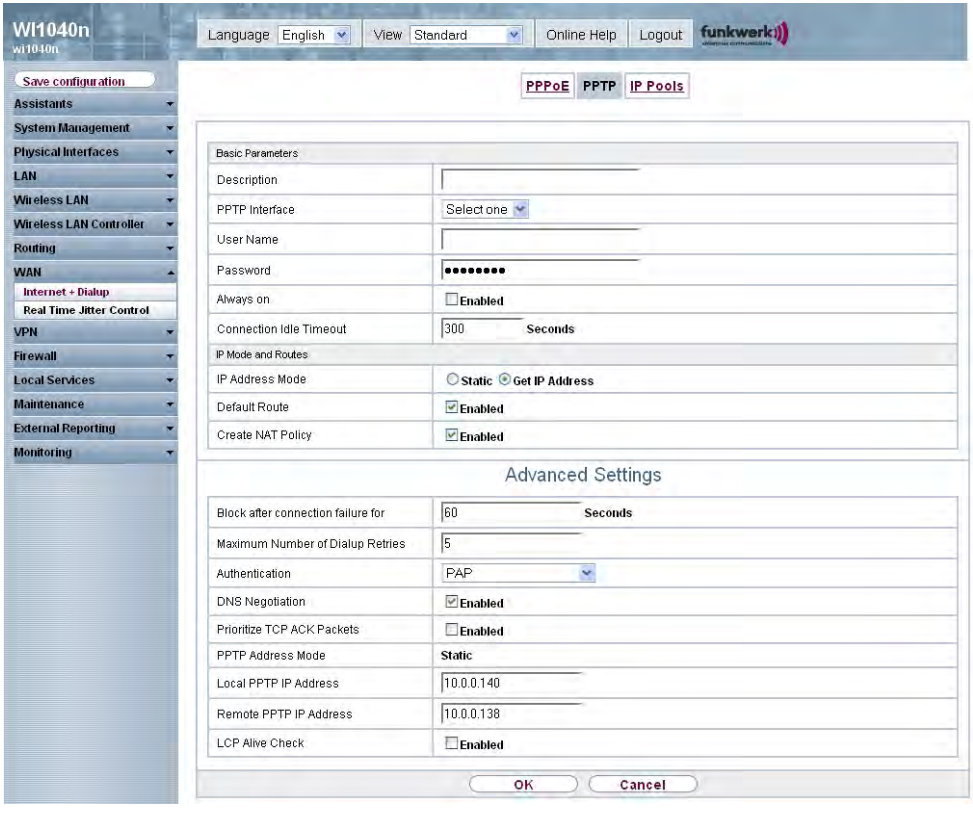


Fig. 108: **WAN -> Internet + Dialup -> PPTP -> New**

The **WAN -> Internet + Dialup -> PPTP -> New** menu consists of the following fields:

Fields in the PPTP Basic Parameters menu

Field	Description
Description	Enter a name for uniquely identifying the internet connection. The first character in this field must not be a number and no special characters or umlauts must be used.
PPTP Interface	Select the IP interface over which packets are to be transported to the remote PPTP terminal.

Field	Description
	If you want to use an external DSL modem, select the Ethernet port to which the modem is connected. When using the internal DSL modem, select here the EthoA interface, e.g. *ethoa50-0*, configured for this connection in **Physical Interfaces**-> **ATM**-> **Profiles**-> **New**. The default value is *Not specified*.
User Name	Enter the user name.
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is activated with *Enabled*. The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle interval in seconds. This determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the timeout. The default value is *300*. Example: *10* for FTP transmission, *20* for LAN-to-LAN transmission, *90* for Internet connections.

Fields in the PPTP IP Mode and Routes menu

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *Get IP Address* (default value): Your device is automatic-

Field	Description
	ally assigned a temporarily valid IP address from the provider. • *Static*: You enter a static IP address.
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is activated with *Enabled*. The function is enabled by default.
Create NAT Policy	Specify whether Network Address Translation (NAT) is to be activated. The function is activated with *Enabled*. The function is enabled by default.
Local IP Address	Only for **IP Address Mode** = *Static* Assign an IP address from your LAN to the PPT interface, which is to be used as your device's internal source address.
Route Entries	Only if **IP Address Mode** = *Static* Define other routing entries for this PPTP partner. Add a new entry with **Add**. • *Remote IP Address*: IP address of the destination host or destination network. • *Netmask*: Netmask of **Remote IP Address**. If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (possible values *0*... *15*). The default value is *1*.

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *60*.

Field	Description
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked. Possible values are *0* to *100*. The default value is *5*.
Authentication	Select the authentication protocol for this Internet connection. Select the authentication specified by your provider. Possible values: • *PAP* (default value) Only run *PAP* (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Only run *CHAP* (PPP Challenge Handshake Authentication Protocol as per RFC 1994); the password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP* : Run primarily CHAP, if denied then the authentication protocol required by the PPTP partner (MSCHAP version 1 or 2 possible). • *MS-CHAPv2*: Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
DNS Negotiation	Select whether your device receives IP addresses for **Primary DNS Server** and **Secondary DNS Server** from the connection partner or sends these to the connection partner. The function is activated with *Enabled*. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is activated with *Enabled*. The function is disabled by default.

Field	Description
PPTP Address Mode	Displays the address mode. The value cannot be changed. Possible values: • *Static*: The IP address of the Ethernet port selected in **PPTP Interface** will be used.
Local PPTP IP Address	Assign the PPTP interface an IP address that is used as the source address. The default value is *10.0.0.140*.
Remote PPTP IP Address	Enter the IP address of the PPTP partner. The default value is *10.0.0.138*.
LCP Alive Check	Check whether the reachability of the remote terminal is to be checked by sending LCP echo requests or replies. This makes it possible to switch to a backup connection more quickly in the event of line faults. The function is activated with *Enabled*. The function is disabled by default.

15.1.3 IP Pools

In the **IP Pools** menu a list of all IP pools is displayed.

Your device can operate as a dynamic IP address server for PPP connections. You can use this function by providing one or more pools of IP addresses. These IP addresses can be assigned to dialling-in connection partners for the duration of the connection.

Any host routes entered always have priority over IP addresses from the address pools. This means if an incoming call has been authenticated, your device first checks whether a host route is entered in the routing table for this caller. If not, your device can allocate an IP address from an address pool (if available). If address pools have more than one IP address, you cannot specify which connection partner receives which address. The addresses are initially assigned in order. If a new dial-in takes place within an interval of one hour, an attempt is made to allocate the same IP address assigned to this partner the last time.

Use the **Add** button to set up new IP pools.

Fig. 109: **WAN** -> **Internet + Dialup** -> **IP Pools** -> **Add**

The **WAN** -> **Internet + Dialup** -> **IP Pools** -> **Add** menu consists of the following fields:

Fields in the Internet + Dialup IP Pools menu

Field	Description
IP Pool Name	Enter the name of the IP pool.
IP Pool Range	In the first field, enter the first IP address of the range. In the second field, enter the last IP address of the range.

15.2 Real Time Jitter Control

When telephoning over the Internet, voice data packets normally have the highest priority. Nevertheless, if the upstream bandwidth is low, noticeable delays in voice transmission can occur when other packets are routed at the same time.

The real time jitter control function solves this problem. So that the "line" is not blocked for too long for the voice data packets, the size of the other packets can be reduced, if required, during a telephone call.

15.2.1 Controlled Interfaces

In the **WAN** -> **Real Time Jitter Control** ->**Controlled Interfaces** menu, a list of all interfaces is shown for which the real time jitter control has been configured.

15.2.1.1 New

Click o the **New** button to set up port forwarding for other interfaces.

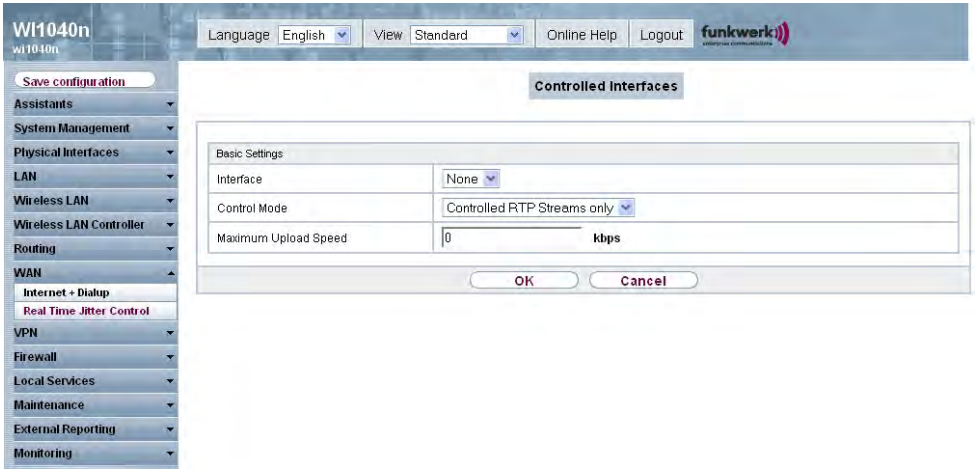


Fig. 110: **WAN -> Real Time Jitter Control -> Controlled Interfaces -> New**

The **WAN -> Real Time Jitter Control -> Controlled Interfaces -> New** menu consists of the following fields:

Fields in the Controlled Interfaces Basic Settings menu

Field	Description
Interface	Define for which interfaces voice transmission is to be optimised.
Control Mode	Select the mode for the optimisation. Possible values: • *Only Controlled RTP Streams*(default value): By means of the data routed via the media gateway, the system detects voice data traffic and optimises the voice transmission. • *All RTP Streams*: All RTP streams are optimised. • *Down* : Voice data transmission is not optimised. • *Always*: Voice data transmission is always optimised.
Maximum Upload Speed	Enter the maximum available upstream bandwidth in kbps for

Field	Description
	the selected interface.

Chapter 16 VPN

A connection that uses the Internet as a "transport medium" but is not publicly accessible is referred to as a VPN (Virtual Private Network). Only authorised users have access to such a VPN, which is seemingly also referred to as a VPN tunnel. Normally the data transported over a VPN is encrypted.

A VPN allows field staff or staff working from home offices to access data on the company's network. Subsidiaries can also connect to head office over VPN.

Various protocols are available for creating a VPN tunnel, e.g. IPSec or PPTP.

The connection partner is authenticated with a password, using preshared keys or certificates.

With IPSec the data is encrypted using AES or 3DES, for example; with PPTP, you can use MPPE.

16.1 IPSec

IPSec enables secure connections to be set up between two locations (VPN). This enables sensitive business data to be transferred via an unsecure medium such as the Internet. The devices used function here as the endpoints of the VPN tunnel. IPSec involves a number of Internet Engineering Task Force (IETF) standards, which specify mechanisms for the protection and authentication of IP packets. IPSec offers mechanisms for encrypting and decrypting the data transferred in the IP packets. The IPSec implementation can also be smoothly integrated in a Public Key Infrastructure (PKI, see *Certificates* on page 112). The funkwerk IPSec implementation achieves this firstly by using the Authentication Header (AH) protocol and Encapsulated Security Payload (ESP) protocol, and secondly through the use of cryptographic key key administration mechanisms like the Internet Key Exchange (IKE) protocol.

16.1.1 IPSec Peers

An endpoint of a communication is defined as peer in a computer network. Each peer offers its services and uses the services of other peers.

In the **VPN** -> **IPSec** -> **IPSec Peers** menu a list of all configured IPSec peers is shown.

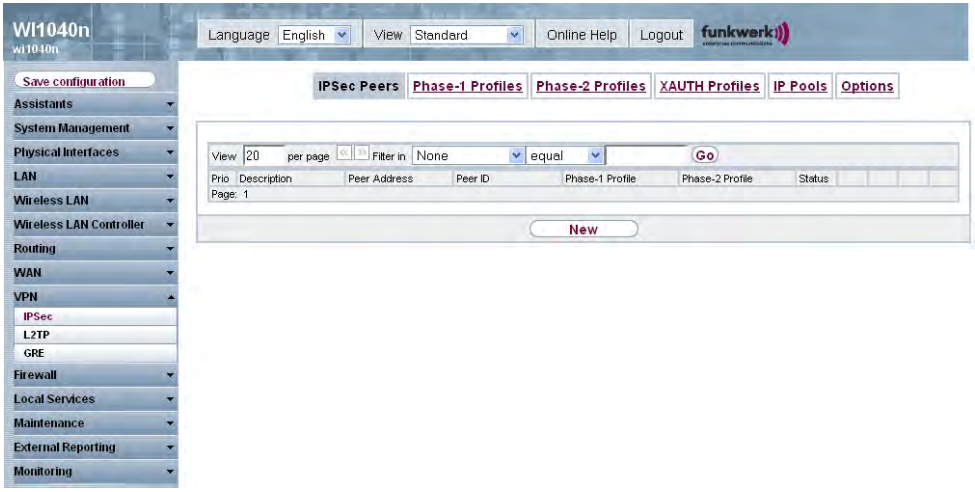


Fig. 111: **VPN -> IPSec -> IPSec Peers**

Peer Monitoring

The menu for monitoring a peer is called by selecting the button for the peer in the peer list. See *Values in the list IPSec Tunnels* on page 391.

16.1.1.1 New

Choose the **New** button to set up more IPSec peers.

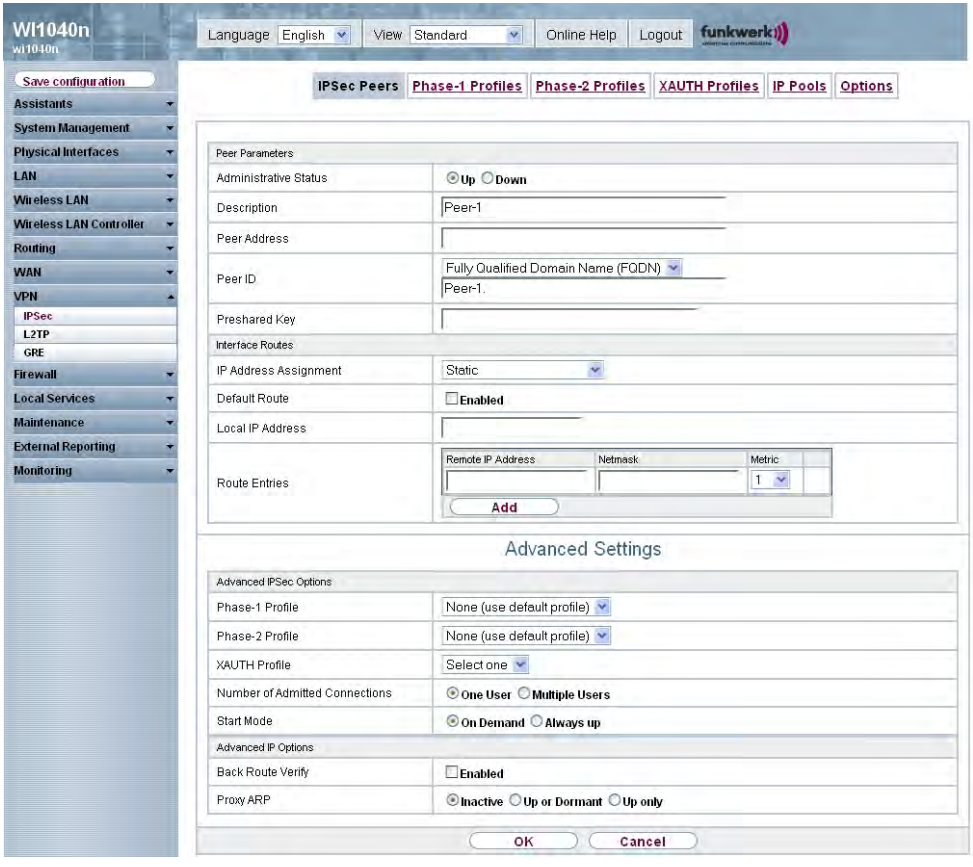


Fig. 112: **VPN** -> **IPSec** -> **IPSec Peers** -> **New**

The **VPN** -> **IPSec** -> **IPSec Peers** -> **New** menu consists of the following fields:

Fields in the IPSec Peers Peer Parameters menu

Field	Description
Administrative Status	Select the status to which you wish to set the peer after saving the peer configuration. Possible values: • *Up* (default value): The peer is available for setting up a tunnel immediately after saving the configuration. • *Down* : The peer is initially not available after the configuration has been saved.
Description	Enter a description of the peer that identifies it.

Field	Description
	The maximum length of the entry is 255 characters.
Peer Address	Enter the official IP address of the peer or its resolvable host name. The entry can be omitted in certain configurations, whereby your device then cannot initiate an IPSec connection.
Peer ID	Select the ID type and enter the peer ID. This entry is not necessary in certain configurations. The maximum length of the entry is 255 characters. Possible ID types: • *Fully Qualified Domain Name (FQDN)* • *E-mail Address* • *IPV4 Address* • *ASN.1-DN (Distinguished Name)* On the peer device, this ID corresponds to the parameter **Local ID Value**.
Preshared Key	Enter the password agreed with the peer. The maximum length of the entry is 50 characters. All characters are possible except for *0x* at the start of the entry.

Fields in the IPSec Peers Interface Routes menu

Field	Description
IP Address Assignment	Select the configuration mode of the interface. Possible values: • *Static* (default value): Enter a static IP address. • *IKE Config Mode Client*: Select this option if your gateway receives an IP address from the server as IPSec client. • *IKE Config Mode Server*: Select this option if your gateway assigns an IP address as DHCP server for connecting clients. This is taken from the selected **IP Assignment Pool**.

Field	Description
IP Assignment Pool	Only if **IP Address Assignment** = *IKE Config Mode Server* Select an IP pool configured in the **VPN** -> **IP Pools** menu. If an IP pool has not been configured here yet, the message *Not yet defined* appears in this field.
Default Route	Only for **IP Address Assignment** = *Static* Select whether the route to this IPSec peer is to be defined as the default route. The function is activated with *Enabled*. The function is disabled by default.
Local IP Address	Only if **IP Address Assignment** = *Static* and *IKE Config Mode Server* Enter the WAN IP address of your IPSec tunnel. This can be the same IP address as the address configured on your router as the LAN IP address.
Route Entries	Define routing entries for this connection partner. • *Remote IP Address*: IP address of the destination host or LAN. • *Netmask*: Netmask of **Remote IP Address**. • *Metric*: The lower the value, the higher the priority of the route (possible values *0...15*). The default value is *1*.

The **Advanced Settings** menu consists of the following fields:

Fields in the Advanced Settings Advanced IPSec Options menu

Field	Description
Phase 1 Profile	For phase 1, select a profile already configured in the **Phase-1 Profiles** menu. You can also select the profile marked as the default in **Phase-1 Profiles**: *None (use Default Profile)*.
Phase 2 Profile	For phase 2, select a profile already configured in the **Phase-2 Profiles** menu. You can also select the profile marked as the

Field	Description
	default in **Phase-2 Profiles**: *None (use Default Profile)*.
XAUTH Profile	Select a profile created in **VPN** -> **IPSec** -> **XAUTH profiles** if you wish to use this IPSec peer XAuth for authentication. If XAuth is used together with IKE Config Mode, the transactions for XAuth are carried out before the transactions for IKE Config Mode.
Number of Admitted Connections	Choose how many users can connect using this peer profile. Possible values: • *One User* (default value): Only one peer can be connected with the data defined in this profile. • *Multiple Users*: Several peers can be connected with the data defined in this profile. The peer entry is duplicated for each connection request with the data defined in this profile.
Start Mode	Select how the peer is to be switched to the active state. Possible values: • *On Demand* (default value): The peer is switched to the active state by a trigger. • *Always on*: The peer is always active.

Fields in the Advanced Settings Advanced IP Options menu

Field	Description
Back Route Verify	Select whether a check on the back route should be activated for the interface to the connection partner. The function is activated with *Enabled*. The function is disabled by default.
Proxy ARP	Select whether your device is to respond to ARP requests from its own LAN on behalf of the specific connection partner. Possible values: • *Inactive* (default value): Deactivates Proxy ARP for this IPSec peer.

Field	Description
	• *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the IPSec peer is *Up* (active) or *Dormant*. In the case of *Idle*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up Only*: Your device responds to an ARP request only if the status of the connection to the IPSec peer is *Up* (active), i.e. a connection already exists to the IPSec peer.

16.1.2 Phase-1 Profiles

In the **VPN** -> **IPSec** -> **Phase-1 Profiles** menu a list of all configured IPSec phase-1 profiles is shown.

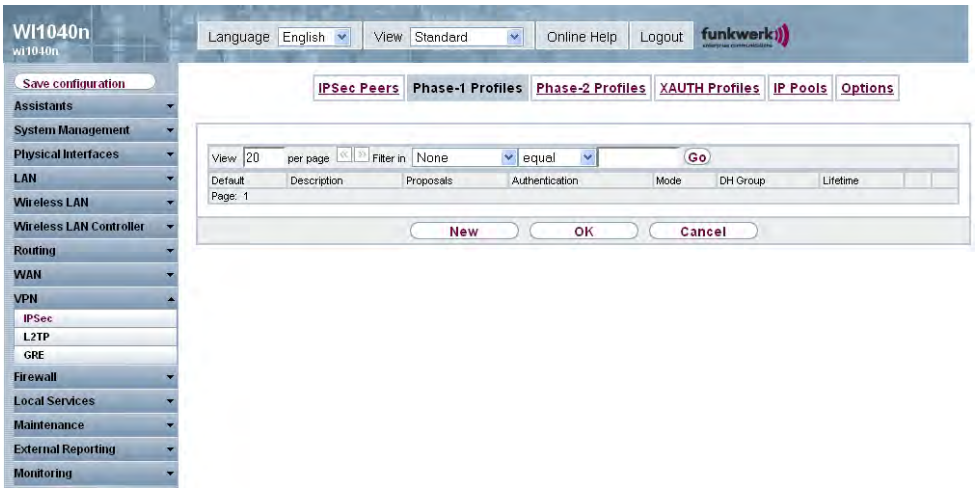


Fig. 113: **VPN** -> **IPSec** -> **Phase-1 Profiles**

In the **Standard** column, you can mark the profile to be used as the default profile.

16.1.2.1 New

Choose the **New** button to set up new profiles.

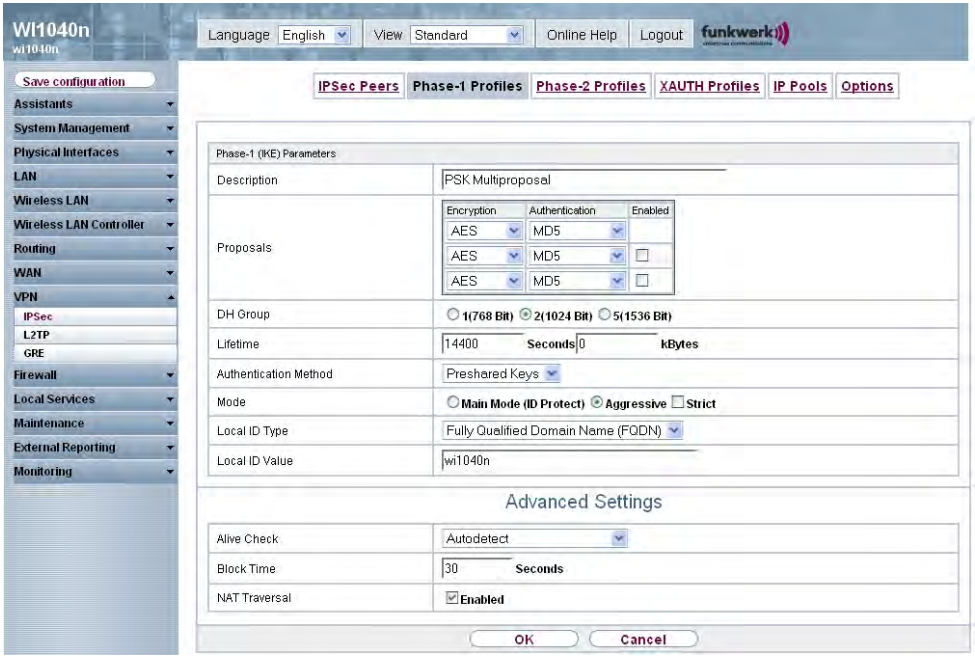


Fig. 114: **VPN -> IPSec ->Phase-1 Profiles -> New**

The **VPN -> IPSec -> Phase-1 Profiles-> New** menu consists of the following fields:

Fields in the Phase-1 Profiles Phase-1 (IKE) Parameters menu

Field	Description
Description	Enter a description that uniquely defines the type of rule.
Proposals	In this field, you can select any combination of encryption and message hash algorithms for IKE phase 1 on your device. The combination of six encryption algorithms and four message hash algorithms gives 24 possible values in this field. At least one proposal must exist. Therefore the first line of the table cannot be deactivated. Encryption algorithms (**Encryption**): • *3DES* (default value): 3DES is an extension of the DES algorithm with an effective key length of 112 bits, which is rated as secure. It is the slowest algorithm currently supported. • *Twofish*: Twofish was a final candidate for the AES (Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower.

Field	Description
	• *Blowfish*: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish. • *CAST*: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES. • *DES*: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits. • *AES*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. • *AES-128*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 128 bits. • *AES-192*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 192 bits. • *AES-256*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 256 bits. Hash algorithms (**Authentication**): • *MD5* (default value): MD 5 (Message Digest #5) is an older hash algorithm. It is used with a 96 bit digest length for IPSec. • *SHA1* : SHA1 (Secure Hash Algorithm #1) is a hash algorithm developed by the NSA (United States National Security Association). It is rated as secure, but is slower than MD5. It is used with a 96 bit digest length for IPSec. • *RipeMD 160*: RipeMD 160 is a 160 bit hash algorithm. It is used as a secure replacement for MD5 and RipeMD. • *Tiger192*: Tiger 192 is a relatively new and very fast algorithm. Please note that the description of the encryption and authentication or the hash algorithms is based on the author's knowledge and opinion at the time of creating this User Guide. In particular, the quality of the algorithms is subject to relative aspects and may change due to mathematical or cryptographic developments.

Field	Description
DH Group	The Diffie-Hellman group defines the parameter set used as the basis for the key calculation during phase 1. "MODP" as supported by **bintec** devices stands for "modular exponentiation". Possible values: • *1 (768 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 768 bits is used to create the encryption material. • *2 (1024 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 1024 bits is used to create the encryption material. • *5 (1536 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 1536 bits is used to create the encryption material.
Lifetime	Create a lifetime for phase 1 keys. As for RFC 2407, the default value is eight hours, which means the key must be renewed once eight hours have elapsed. The following options are available for defining the lifetime: Entry in **Seconds**: Enter the lifetime for phase 1 key in seconds. The value can be a whole number from 0 to 2147483647. The default value is *14400*. Entry in **KBytes**: Enter the lifetime for phase 1 keys as amount of data processed in kBytes. The value can be a whole number from 0 to 2147483647. The default value is *0*. The standard value as per RFC is used *0* seconds and *0* Kbytes are entered.
Authentication Method	Select the authentication method. Possible values: • *Preshared Keys* (default value): If you do not use certificates for the authentication, you can select Preshared Keys. These are configured during peer configuration in the **IPSec Peers** menu. The preshared key is the shared password. • *DSA Signature*: Phase 1 key calculations are authenticated using the DSA algorithm.

Field	Description
	• *RSA Signature*: Phase 1 key calculations are authenticated using the RSA algorithm. • *RSA Encryption*: In RSA encryption the ID payload is also encrypted for additional security.
Local Certificate	Only if **Authentication Method** = *DSA Signature*, *RSA Signature* or *RSA Encryption* This field enables you to select one of your own certificates for authentication. It shows the index number of this certificate and the name under which it is saved. This field is only shown for authentication settings based on certificates and indicates that a certificate is essential.
Mode	Select the phase 1 mode. Possible values: • *Aggressive* (default value): The Aggressive Mode is necessary if one of the peers does not have a static IP address and preshared keys are used for authentication; it requires only three messages for configuring a secure channel. • *Main Mode (ID Protect)* : This mode (also designated Main Mode) requires six messages for a Diffie-Hellman key calculation and thus for configuring a secure channel, over which the IPSec SAs can be negotiated. A condition is that both peers have static IP addresses if preshared keys are used for authentication. Also define whether the selected mode is used exclusively (**Strict**), or the peer can also propose another mode.
Local ID Type	Select the local ID type. Possible values: • *Fully Qualified Domain Name (FQDN)* • *E-mail Address* • *IPV4 Address* • *ASN.1-DN (Distinguished Name)*
Local ID Value	Enter the ID of your device.

Field	Description
	For **Authentication Method** = *DSA Signature*, *RSA Signature* or *RSA Encryption*, the **Use Subject Name from certificate** option is shown. If you enable the **Use Subjectname from Certificate** option, the first alternative subject name indicated in the certificate is used, or, if none is specified, the subject name of the certificate is used. Note: If you use certificates for authentication and your certificate contains alternative subject names (see *Certificates* on page 112), you must make sure your device selects the first alternative subject name by default. Make sure you and your peer both use the same name, i.e. that your local ID and the peer ID your partner configures for you are identical.

Alive Check

During communication between two IPSec peers, one of the peers may become unavailable, e.g. due to routing problems or a reboot. However, this can only be detected when the end of the lifetime of the security connection is reached. Up until this point the data packets are lost. These are various methods of performing an alive check to prevent this happening. In the **Alive Check** field you can specify whether a method should be used to check the availability of a peer.

Two methods are available: Heartbeats and Dead Peer Detection.

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Alive Check	Select the method to be used to check the functionality of the IPSec connection. In addition to the default method Dead Peer Detection (DPD), the (proprietary) Heartbeat method is implemented. This sends and receives signals every 5 seconds, depending on the configuration. If these signals are not received after 20 seconds, the SA is discarded as invalid. Possible values: • *Autodetect* (default value): Your device detects and uses

Field	Description
	the mode supported by the remote terminal. • *Down* : Your device sends and expects no heartbeat. Set this option if you use devices from other manufacturers. • *Heartbeats (Expect only)*: Your device expects a heartbeat from the peer but does not send one itself. • *Heartbeats (Send only)*: Your device expects no heartbeat from the peer, but sends one itself. • *Heartbeats (send & expect)*: Your device expects a heartbeat from the peer and sends one itself. • *Dead Peer Detection*: Use DPD (dead peer detection) in accordance with RFC 3706. DPD uses a request-reply protocol to check the availability of the remote terminal and can be configured independently on both sides. This option only checks the availability of the peer if data is to be sent to it. • *Dead Peer Detection (Idle)*: Use DPD (dead peer detection) in accordance with RFC 3706. DPD uses a request-reply protocol to check the availability of the remote terminal and can be configured independently on both sides. This option is used to carry out a check at certain intervals depending on forthcoming data transfers.
Block Time	Define how long a peer is blocked for tunnel setups after a phase 1 tunnel setup has failed. This only affects locally initiated setup attempts. Possible values are *-1* to *86400* (seconds); *-1* means the value in the default profile is used and *0* means that the peer is never blocked. The default value is *30*.
NAT Traversal	NAT Traversal (NAT-T) also enables IPSec tunnels to be opened via one or more devices on which network address translation (NAT) is activated. Without NAT-T, incompatibilities may arise between IPSec and NAT (see RFC 3715, section 2). These primarily prevent the setup of an IPSec tunnel from a host within a LANs and behind a NAT device to another host or device. NAT-T enables these kinds of tunnels without conflicts with NAT device, activated NAT is automatically detected by the IPSec Daemon and NAT-T

Field	Description
	is used. The function is activated with *Enabled*. The function is enabled by default.
CA Certificates	Only if **Authentication Method** = *DSA Signature*, *RSA Signature* or *RSA Encryption* If you enable the **Trust the following CA certificates** option, you can select up to three additional CA certificates that are accepted for this profile. This option can only be configured if certificates are loaded.

16.1.3 Phase-2 Profiles

You can define profiles for phase 2 of the tunnel setup just as for phase 1.

In the **VPN** -> **IPSec** -> **Phase-2 Profiles** menu a list of all configured IPSec phase-2 profiles is shown.

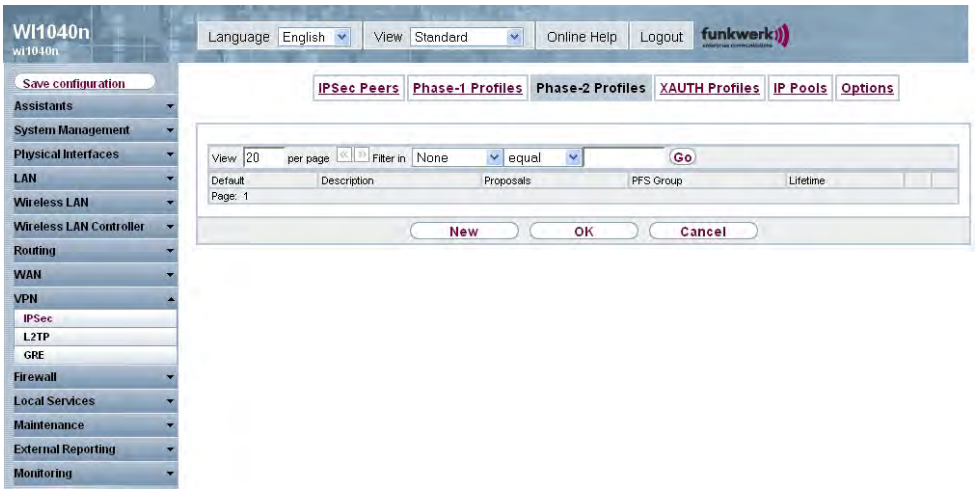


Fig. 115: **VPN** -> **IPSec** -> **Phase-2 Profiles**
In the **Standard** column, you can mark the profile to be used as the default profile.

16.1.3.1 New

Choose the **New** button to set up new profiles.

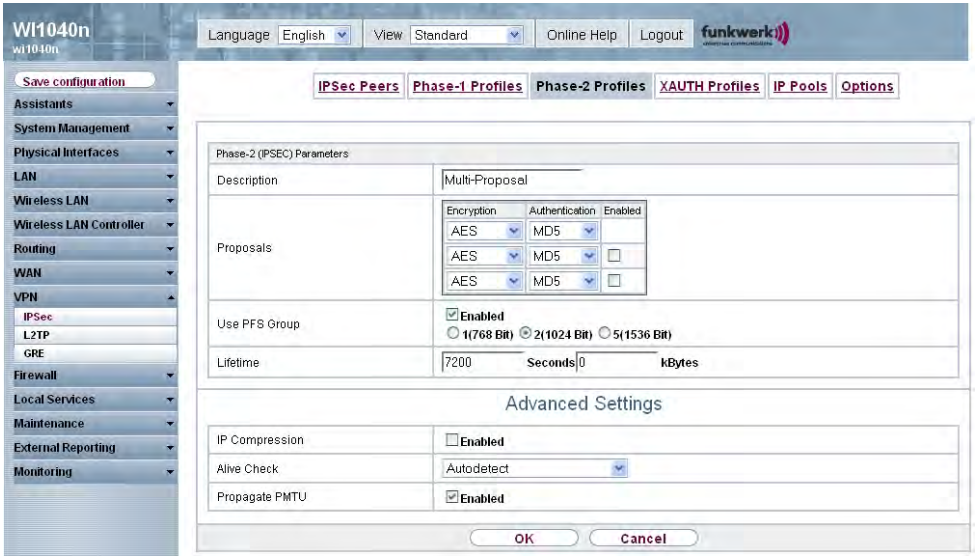


Fig. 116: **VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New**

The **VPN** -> **IPSec** -> **Phase-2 Profiles**-> **New** menu consists of the following fields:

Fields in the Phase-2 Profiles Phase-2 (IPSEC) Parameters menu

Field	Description
Description	Enter a description that uniquely identifies the profile. The maximum length of the entry is 255 characters.
Proposals	In this field, you can select any combination of encryption and message hash algorithms for IKE phase 2 on your default. The combination of six encryption algorithms and two message hash algorithms gives 12 possible values in this field. Encryption algorithms (**Encryption**): • *3DES* (default value): 3DES is an extension of the DES algorithm with an effective key length of 112 bits, which is rated as secure. It is the slowest algorithm currently supported. • *-ALL-*: All options can be used. • *AES-128*: Rijndael has been nominated as AES due to its

Field	Description
	fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 128 bits. • *AES-192*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 192 bits. • *AES-256*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 256 bits. • *Twofish*: Twofish was a final candidate for the AES (Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower. • *Blowfish*: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish. • *CAST*: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES. • *DES*: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits. Hash algorithms (**Authentication**): • *MD 5* (default value): MD 5 (Message Digest #5) is an older hash algorithm. It is used with a 96 bit digest length for IPSec. • *-ALL-*: All options can be used. • *SHA 1* : SHA1 (Secure Hash Algorithm #1) is a hash algorithm developed by the NSA (United States National Security Association). It is rated as secure, but is slower than MD5. It is used with a 96 bit digest length for IPSec. Note that RipeMD 160 and Tiger 192 are not available for message hashing in phase 2.
Use PFS Group	As PFS (Perfect Forward Secrecy) requires another Diffie-Hellman key calculation to create new encryption material, you must select the exponentiation features. If you enable PFS (**Enabled**), the options are the same as for the configuration in **Phase 1: Group**. PFS is used to protect the keys of a renewed phase 2 SA, even if the keys of the phase 1 SA have become known.

Field	Description
	The field has the following options: • *1 (768 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 768 bits is used to create the encryption material. • *2 (1024 Bit)* (default value): During the Diffie-Hellman key calculation, modular exponentiation at 1024 bits is used to create the encryption material. • *5 (1536 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 1536 bits is used to create the encryption material.
Lifetime	Define how the lifetime is defined that will expire before phase 2 SAs need to be renewed. The new SAs are negotiated shortly before expiry of the current SAs. As for RFC 2407, the default value is eight hours, which means the key must be renewed once eight hours have elapsed. The following options are available for defining the lifetime: Entry in *Seconds*: Enter the lifetime for phase 2 key in seconds. The value can be a whole number from *0* to *2147483647*. The default value is *7200*. Entry in *KBytes*: Enter the lifetime for phase 2 keys as amount of data processed in Kbytes. The value can be a whole number from *0* to *2147483647*. The default value is *0*.

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
IP Compression	Select whether compression is to be activated before data encryption. If data is compressed effectively, this can result in higher performance and a lower volume of data to be transferred. In the case of fast lines or data that cannot be compressed, you are advised against using this option as the performance can be significantly affected by the increased effort during compression.

Field	Description
	The function is activated with *Enabled*. The function is disabled by default.
Alive Check	Select whether and how IPSec heartbeats are used. A **bintec** IPSec heartbeat is implemented to determine whether or not a Security Association (SA) is still valid. This function sends and receives signals every 5 seconds, depending on the configuration. If these signals are not received after 20 seconds, the SA is discarded as invalid. Possible values: • *Inactive* : Your device sends and expects no heartbeat. Set this option if you use devices from other manufacturers. • *Heartbeats (Expect only)*: Your device expects a heartbeat from the peer but does not send one itself. • *Heartbeats (Send only)*: Your device expects no heartbeat from the peer, but sends one itself. • *Heartbeats (send & expect)*: Your device expects a heartbeat from the peer and sends one itself. • *Autodetect*: Automatic detection of whether the remote terminal is a **bintec** device. If it is, Heartbeat Both (for a remote terminal with **bintec**) or None (for a remote terminal without **bintec**) is set.
Propagate PMTU	Select whether the PMTU (Path Maximum Transfer Unit) is to be propagated during phase 2. The function is activated with *Enabled*. The function is enabled by default.

16.1.4 XAUTH Profiles

In the **XAUTH Profiles** menu a list of all XAuth users is displayed.

Extended Authentication for IPSec (XAuth) is an additional authentication method for IPSec tunnel users.

The gateway can take on two different roles when using XAuth as it can act as a server or

as a client:

- As a server the gateway requires a proof of authorisation.
- As a client the gateway provides proof of authorisation.

In server mode multiple users can obtain authentication via XAuth, e.g. users of Apple iPhones. Authorisation is verified either on the basis of a list or via a Radius Server. If using a one time password (OTP), the password check can be carried out by a token server (e.g. SecOVID from Kobil), which is installed behind the Radius Server. If a company's headquarters is connected to several branches via IPSec, several peers can be configured. A specific user can then use the IPSec tunnel over various peers depending on the assignment of various profiles. This is useful, for example, if an employee works alternately in different branches, if each peer represents a branch and if the employee wishes to have on-site access to the tunnel.

XAuth is carried out once IPSec IKE (Phase 1) has been completed successfully and before IKE (Phase 2) begins.

If XAuth is used together with IKE Config Mode, the transactions for XAuth are carried out before the transactions for IKE Config Mode.

16.1.4.1 New

Choose the **New** button to set up new profiles.

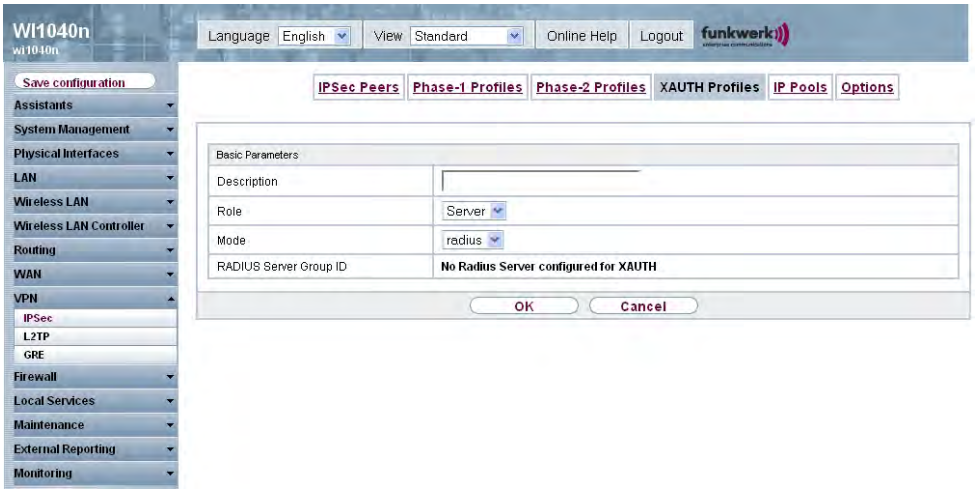


Fig. 117: **VPN** -> **IPSec** -> **XAUTH Profiles** -> **New**

The **VPN** -> **IPSec** -> **XAUTH Profiles** -> **New** menu consists of the following fields:

Fields in the XAUTH Profiles Basic Parameters menu

Field	Description
Description	Enter a description for this XAuth profile.
Role	Select the role of the gateway for XAuth authentication. Possible values: • *Server* (default value): The gateway requires a proof of authorisation. • *Client*: The gateway provides proof of authorisation.
Mode	Only if **Role** = *Server* Select how authentication is carried out. Possible values: • *RADIUS* (default value): Authentication is carried out via a Radius server. This is configured in the **System Management** -> **Remote Authentication** -> **RADIUS** menu and selected in the **RADIUS Server Group ID** field. • *Local*: Authentication is carried out via a local list.
Name	Only if **Role** = *Client* Enter the authentication name of the client.
Password	Only if **Role** = *Client* Enter the authentication password.
RADIUS Server Group ID	Only if **Role** = *Server* Select the desired RADIUS group configured in **System Management** -> **Remote Authentication** -> **RADIUS**.
Users	Only if **Role** = *Server* and **Mode** = *Local* If your gateway is configured as an XAuth server, the clients can be authenticated via a locally configured user list. Define the members of the user group of this XAUTH profile here by entering the authentication name of the client (**Name**) and the authentication password (**Password**). Add new members with **Add**.

16.1.5 IP Pools

In the **IP Pools** menu a list of all IP pools for your configured IPSec connections is displayed.

If have set **IP Address Assignment** *IKE Config Mode Server* for an IPSec peer, you must define the IP pools from which the IP addresses are assigned.

Use the **Add** button to set up new IP pools.

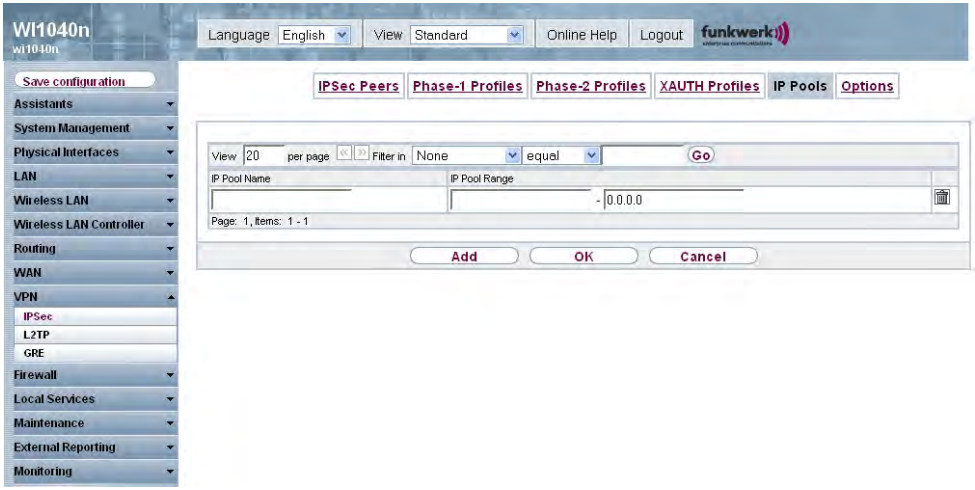


Fig. 118: **VPN** -> **IPSec** -> **IP Pools** -> **Add**

The **VPN** -> **IPSec** -> **IP Pools** -> **Add** menu consists of the following fields:

Fields in the Options IP Pools menu

Field	Description
IP Pool Name	Enter the name of the IP pool.
IP Pool Range	In the first field, enter the first IP address of the range. In the second field, enter the last IP address of the range.

16.1.6 Options

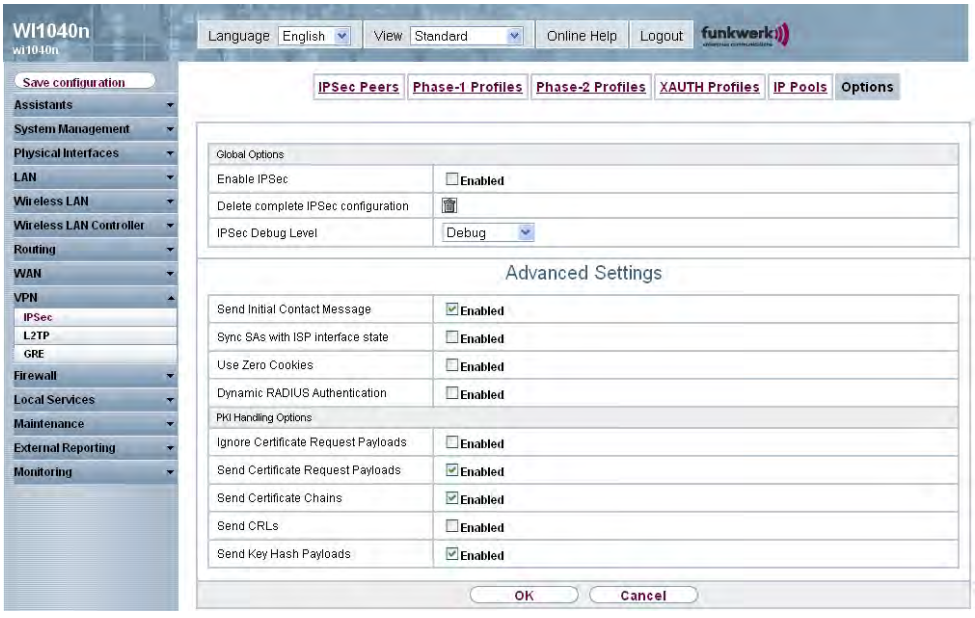


Fig. 119: **VPN** -> **IPSec** -> **Options**

The **VPN** -> **IPSec** -> **Options** menu consists of the following fields:

Fields in the Options Global Options menu

Field	Description
Enable IPSec	Select whether you want to activate IPSec. The function is activated with *Enabled*. The function is active as soon as an IPSec Peer is configured.
Delete complete IPSec configuration	If you click the icon, delete the complete IPSec configuration of your device. This cancels all settings made during the IPSec configuration. Once the configuration is deleted, you can start with a completely new IPSec configuration. You can only delete the configuration if **Enable IPSec** = *Not activated*.

Field	Description
IPSec Debug Level	Select the priority of the syslog messages of the IPSec subsystem to be recorded internally. Possible values: • *Emergency* (highest priority) • *Alert* • *Critical* • *Error* • *Warning* • *Notice* • *Information* • *Debug* (default value, lowest priority) Syslog messages are only recorded internally if they have a higher or identical priority to that indicated, i.e. all messages generated are recorded at syslog level debug.

The **Advanced Settings** menu is for adapting certain functions and features to the special requirements of your environment, i.e. mostly interoperability flags are set. The default values are globally valid and enable your system to work correctly to other **bintec** devices, so that you only need to change these values if the remote terminal is a third-party product or you know special settings are necessary. These may be needed, for example, if the remote end operates with older IPSec implementations.

The **Advanced Settings** menu consists of the following fields:

Fields in the Options Advanced Settings menu

Field	Description
Send Initial Contact Message	Select whether IKE Initial Contact messages are to be sent during IKE (phase 1) if no SAs with a peer exist. The function is activated with *Enabled*. The function is enabled by default.
Sync SAs with ISP interface state	Select whether all SAs are to be deleted whose data traffic was routed via an interface on which the status has changed from *Up*to *Down*, *Dormant* or *Blocked*. The function is activated with *Enabled*.

Field	Description
	The function is disabled by default.
Use Zero Cookies	Select whether zeroed ISAKMP Cookies are to be sent. These are equivalent to the SPI (Security Parameter Index) in IKE proposals; as they are redundant, they are normally set to the value of the negotiation currently in progress. Alternatively, your device can use zeroes for all values of the cookie. In this case choose *Enabled*.
Zero Cookie Size	Only if **Use Zero Cookies** = activated. Enter the length in bytes of the zeroed SPI used in IKE proposals. The default value is *32*.
Dynamic RADIUS Authentication	Select whether RADIUS authentication is to be activated via IPSec. The function is activated with *Enabled*. The function is disabled by default.

Fields in the Advanced Settings PKI Handling Options menu

Field	Description
Ignore Certificate Request Payloads	Select whether certificate requests received from the remote end during IKE (phase 1) are to be ignored. The function is activated with *Enabled*. The function is disabled by default.
Send Certificate Request Payloads	Select whether certificate requests are to be sent during IKE (phase 1). The function is activated with *Enabled*. The function is enabled by default.
Send Certificate Chains	Select whether complete certificate chains are to be sent during IKE (phase 1). The function is activated with *Enabled*.

Field	Description
	The function is enabled by default. Deactivate this function if you do not wish to send the peer the certificates of all levels (from your level to the CA level).
Send CRLs	Select whether CRLs are to be sent during IKE (phase 1). The function is activated with *Enabled*. The function is disabled by default.
Send Key Hash Payloads	Select whether key hash payloads are to be sent during IKE (phase 1). In the default setting, the public key hash of the remote end is sent together with the other authentication data. Only applies for RSA encryption; activate this function with *Enabled* to suppress this behaviour.

16.2 L2TP

The layer 2 tunnel protocol (L2TP) enables PPP connections to be tunnelled via a UDP connection.

Your **bintec** device supports the following two modes:

- L2TP LNS Mode (L2TP Network Server): for incoming connections only
- L2TP LAC Mode (L2TP Access Concentrator): for outgoing connections only

Note the following when configuring the server and client: An L2TP tunnel profile must be created on each of the two sides (LAC and LNS). The corresponding L2TP tunnel profile is used on the initiator side (LAC) to set up the connection. The L2TP tunnel profile is needed on the responder side (LNS) to accept the connection.

16.2.1 Tunnel Profiles

In the **VPN** -> **L2TP** -> **Tunnel Profiles** menu a list of all configured tunnel profiles is shown.

16.2.1.1 New

Choose the **New** button to set up new tunnel profiles.

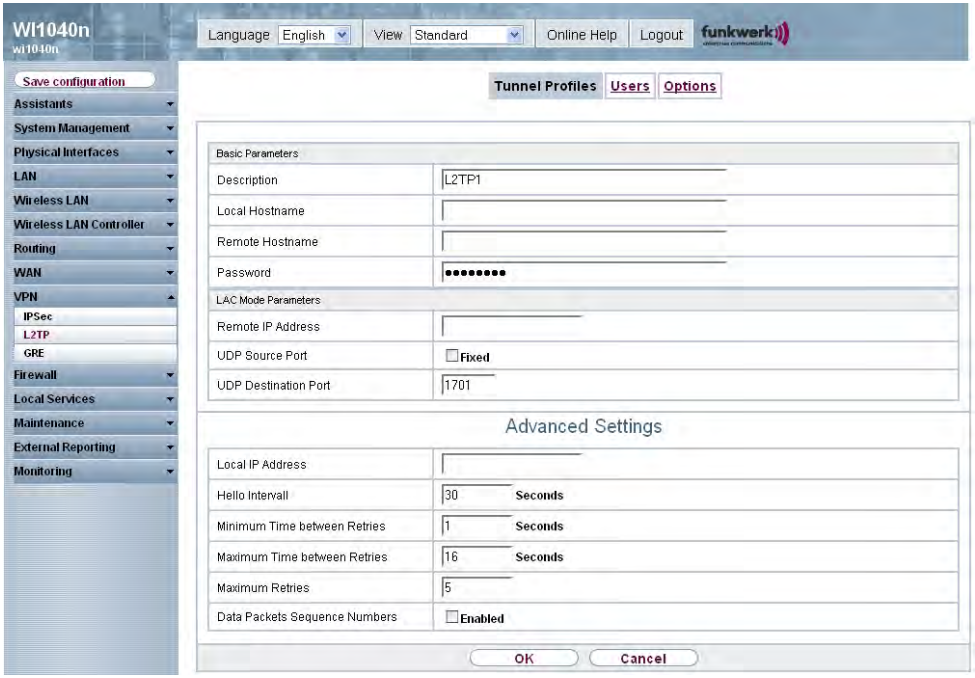


Fig. 120: **VPN** -> **L2TP** -> **Tunnel Profiles** -> **New**

The **VPN** -> **L2TP** -> **Tunnel Profiles** -> **New** menu consists of the following fields:

Fields in the Tunnel Profiles Basic Parameters menu

Field	Description
Description	Enter a description for the current profile. The device automatically names the profiles `L2TP` and numbers them, but the value can be changed.
Local Hostname	Enter the host name for LNS or LAC. • LAC: The **Local Hostname** is used in outgoing tunnel setup messages to identify this device and is associated with the **Remote Hostname** of a tunnel profile configured on the LNS. These tunnel setup messages are SCCRQs (Start Control Connection Request) sent from the LAC and SCCRPs (Start Control Connection Reply) sent from the LNS. • LNS: Is the same as the value for **Remote Hostname** of the incoming tunnel setup message from the LAC.

Field	Description
Remote Hostname	Enter the host name of the LNS or LAC. • LAC: Defines the value for **Local Host Name** of the LNS (contained in the SCCRQs received from the LNS and the SCCRPs received from the LAC). The **Local Hostname** configured in the LAC must match the **Remote Hostname** configured for the intended profile in the LNS and vice versa. • LNS: Defines the **Local Host Name** of the LAC. If the **Remote Hostname** field remains empty on the LNS, the related profile qualifies as the standard entry and is used for all incoming calls for which a profile with a matching **Remote Hostname** can be found.
Password	Enter the password to be used for tunnel authentication. Authentication between LAC and LNS takes place in both directions, i.e. the LNS checks the **Local Hostname** and the **Password** contained in the SCCRQ of the LAC and compares them with those specified in the relevant profile. The LAC does the same with the fields of the SCCRP of the LNS. If this field remains empty, authentication data in the tunnel setup messages are not sent and are ignored.

Fields in the Tunnel Profiles LAC Mode Parameters menu

Field	Description
Remote IP Address	Enter the fixed IP address of the LNS used as the destination address for connections based on this profile. The destination must be a device that can behave like an LNS.
UDP Source Port	Enter how the port number to be used as the source port for all outgoing L2TP connections based on this profile is to be be determined. By default, the **Fixed** option is disabled, which means that ports are dynamically assigned to the connections that use this profile. If you want to enter a fixed port, enable the **Fixed** option. Select this option if you encounter problems with the firewall or NAT. The available values are *0* to *65535*.

Field	Description
UDP Destination Port	Enter the destination port number to be used for all calls based on this profile. The remote LNS that receives the call must monitor this port on L2TP connections. Possible values are *0* ... *65535*. The default value is *1701* (RFC 2661).

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Local IP Address	Enter the IP address to be used as the source address for all L2TP connections based on this profile. If this field is left empty, your device uses the IP address of the interface used to reach **Remote IP Address** by the L2TP tunnel.
Hello Interval	Enter the interval (in seconds) between the sending of two L2TP HELLO messages. These messages are used to keep the tunnel open. The available values are *0* to *255*, the default value is *30*. The value *0* means that no L2TP HELLO messages are sent.
Minimum Time between Retries	Enter the minimum time (in seconds) that your device waits before resending a L2TP control packet for which it received no response. The wait time is dynamically extended until it reaches the **Maximum Time between Retries**. The available values are *1* to *255*, the default value is *1*.
Maximum Time between Retries	Enter the maximum time (in seconds) that your device waits before resending a L2TP control packet for which it received no response. The available values are *8* to *255*, the default value is *16*.
Maximum Retries	Enter the maximum number of times your device is to try to resend the L2TP control packet for which is received no response.

Field	Description
	The available values are *8* to *255*, the default value is *5*.
Data Packets Sequence Numbers	Select whether your device is to use sequence numbers for data packets sent through a tunnel on the basis of this profile. The function is not currently used. The function is activated with *Enabled*. The function is disabled by default.

16.2.2 Users

In the **VPN** -> **L2TP** -> **Users** menu a list of all configured L2TP partners is shown.

16.2.2.1 New

Choose the **New** button to set up new L2TP partners.

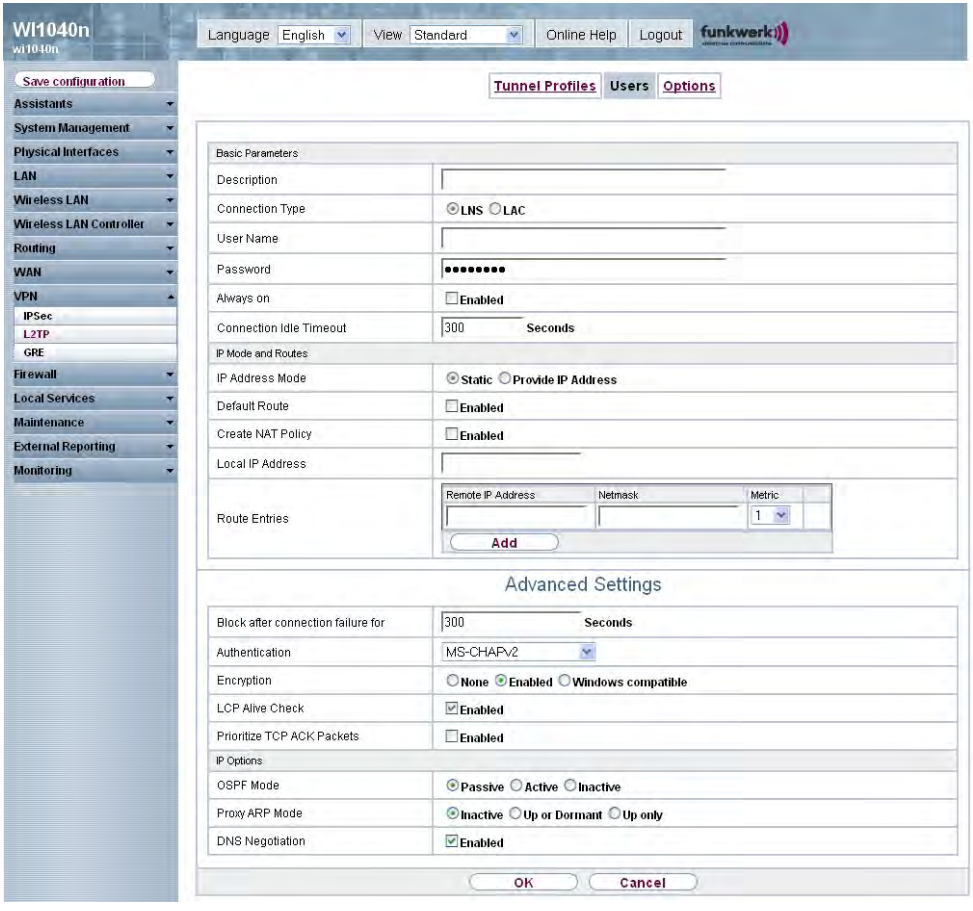


Fig. 121: **VPN** -> **L2TP** -> **Users** -> **New**

The **VPN** -> **L2TP** -> **Users** -> **New** menu consists of the following fields:

Fields in the Users Basic Parameters menu

Field	Description
Description	Enter a name for uniquely identifying the L2TP partner. The first character in this field must not be a number and no special characters or umlauts must be used. The maximum length of the entry is 25 characters.
Connection Type	Select whether the L2TP partner is to take on the role of the L2TP network server (LNS) or the functions of a L2TP access concentrator client (LAC client).

Field	Description
	Possible values: • *LNS* (default value): If you select this option, the L2TP partner is configured so that it accepts L2TP tunnels and restores the encapsulated PPP traffic flow. • *LAC*: If you select this option, the L2TP partner is configured so that it encapsulates a PPP traffic flow in L2TP and sets up a L2TP tunnel to a remote LNS.
Tunnel Profile	Only for **Connection Type** = *LAC* Select a profile created in the **Tunnel Profiles** menu for the connection to this L2TP partner.
User Name	Enter the code of your device.
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is activated with *Enabled*. The function is disabled by default.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the short hold. The default value is *300*.

Fields in the Users IP Mode and Routes menu

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *Static* (default value): You enter a static IP address. • *Provide IP Address*: Only for **Connection Type** = *LNS*

Field	Description
	Your device dynamically assigns an IP address to the remote terminal. • *Get IP Address*: Only for **Connection Type** = *LAC* Your device is dynamically assigned an IP address.
Default Route	Only if **IP Address Mode** = *Get IP Address* and *Static* Select whether the route to this connection partner is to be defined as the default route. The function is activated with *Enabled*. The function is disabled by default.
Create NAT Policy	Only if **IP Address Mode** = *Get IP Address* and *Static* Specify whether Network Address Translation (NAT) is to be activated for this connection. The function is activated with *Enabled*. The function is disabled by default.
IP Assignment Pool (IPCP)	Only if **IP Address Mode** = *Provide IP Address* Select an IP pool configured in the **WAN** -> **Internet + Dialup** -> **IP Pools** menu.
Local IP Address	Only for **IP Address Mode** = *Static* Enter the WAN IP address of your device.
Route Entries	Only for **IP Address Mode** = *Static* Enter the **Remote IP Address** and **Netmask** of the L2TP partner LAN and the corresponding **Metric**. Add new entries with **Add**.

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *300*.
Authentication	Select the authentication protocol for this L2TP partner. Possible values: • *PAP/CHAP/MS-CHAP* (default value): Primarily run CHAP, on denial, the authentication protocol required by the PPTP partner. (MSCHAP version 1 or 2 possible.) • *PAP*: Only run *PAP* (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Only run *CHAP* (PPP Challenge Handshake Authentication Protocol as per RFC 1994); the password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *MS-CHAPv2*: Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
Encryption	If necessary, select the type of encryption that should be used for data traffic to the L2TP partner. This is only possible if STAC or MS-STAC compression is not activated for the connection. If **Encryption** is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values: • *None*: MPP encryption is not used. • *Enabled* (default value): MPP encryption V2 with 128 bit is used to RFC 3078. • *Windows compatible*: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
LCP Alive Check	Check whether the reachability of the remote terminal is to be checked by sending LCP echo requests or replies. This is recommended for leased lines, PPTP and L2TP connections.

Field	Description
	The function is activated with *Enabled*. The function is disabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is activated with *Enabled*. The function is disabled by default.

Fields in the Advanced Settings IP Options menu

Field	Description
OSPF Mode	Select whether and how routes are propagated via the interface and/or OSPF protocol packets are to be sent. Possible values: • *Passive* (default value): OSPF is not activated for this interface, i.e. no routes are propagated or OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces. • *Active*: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface. • *Inactive* : OSPF is disabled for this interface.
Proxy ARP Mode	Select whether your device is to respond to ARP requests from its own LAN on behalf of the specific L2TP partner. Possible values: • *Inactive* (default value): Deactivates Proxy ARP for this L2TP partner. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the L2TP partner is *Up* (active) or *Dormant*. In the case of *Dormant*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up Only*: Your device responds to an ARP request only if the status of the connection to the L2TP partner is *Up* (active), i.e.

Field	Description
	a connection already exists to the L2TP partner.
DNS Negotiation	Select whether your device receives IP addresses for **Primary DNS Server, Secondary DNS Server, primary WINS** and **secondary WINS** from the L2TP partner or sends these to the L2TP partner. The function is activated with *Enabled*. The function is enabled by default.

16.2.3 Options

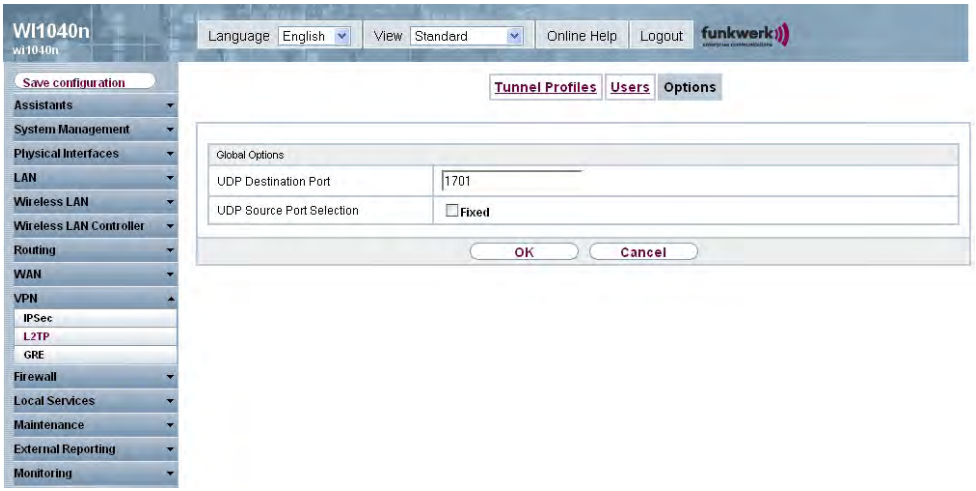


Fig. 122: **VPN** -> **L2TP** -> **Options**

The **VPN** -> **L2TP** -> **Options** menu consists of the following fields:

Fields in the Options Global Options menu

Field	Description
UDP Destination Port	Enter the port to be monitored by the LNS on incoming L2TP tunnel connections. Available values are all whole numbers from *1* to *65535*, the default value is *1701*, as specified in RFC 2661.
UDP Source Port Selec-	Select whether the LNS should only use the monitored port

Field	Description
tion	**UDP destination port**) as the local source port for the L2TP connection. The function is activated with *Fixed*. The function is disabled by default.

16.3 GRE

Generic Routing Encapsulation (GRE) is a network protocol that encapsulates other protocols and transports them in the form of IP tunnels to the specified recipients.

The specification of the GRE protocol is available in two versions:

- GRE V.1 for use in PPTP connections (RFC 2637, configuration in the **PPTP** menu)
- GRE V.0 (RFC 2784) for general encapsulation using GRE

In this menu you can configure a virtual interface for using GRE V.0. The data traffic routed over this interface is then encapsulated using GRE and sent to the specified recipient.

16.3.1 GRE Tunnels

In the **VPN** -> **GRE** -> **GRE Tunnels** menu, a list of all configured GRE tunnels is shown.

16.3.1.1 New

Choose the **New** button to set up new GRE tunnels.

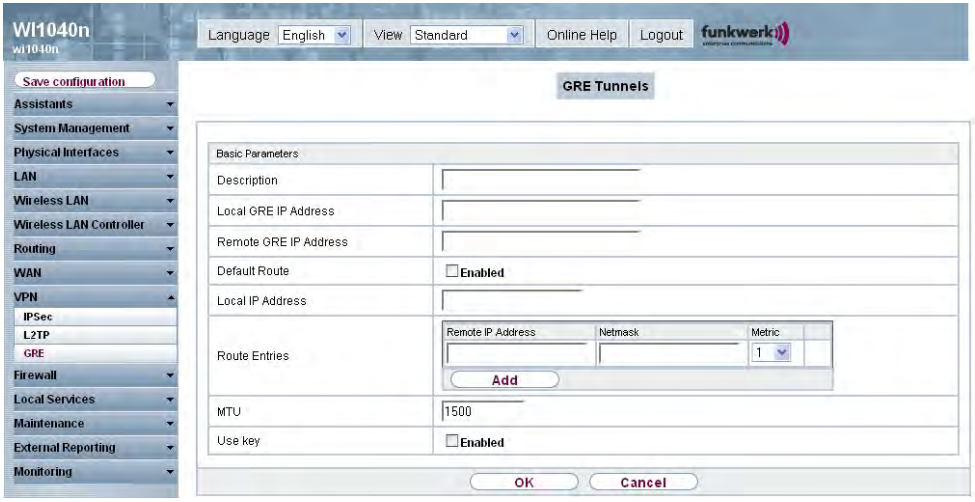


Fig. 123: **VPN** -> **GRE** -> **GRE Tunnels**

The **VPN** -> **GRE** -> **GRE Tunnels** menu consists of the following fields:

Fields in the GRE Tunnels Basic Parameters menu

Field	Description
Description	Enter a description for the GRE tunnel.
Local GRE IP Address	Enter the source IP address of the GRE packets to the GRE partner. If no IP address is given (this corresponds to IP address 0.0.0.0), the source IP address of the GRE packets is selected automatically from one of the addresses of the interface via which the GRE partner is reached.
Remote GRE IP Address	Specify the destination IP address of the host or network to which the packets are to be sent through the GRE tunnel.
Default Route	If you enable the **Default Route**, all data is automatically routed to one connection. The function is disabled by default.
Local IP Address	Enter the IP address to be used as the source address for this GRE connection.

Field	Description
Route Entries	Define other routing entries for this connection partner. Add a new entry with **Add**. • *Remote IP Address*: IP address of the destination host or network. • *Netmask*: Netmask of **Remote IP Address**. If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (possible values *0*... *15*). The default value is *1*.
MTU	Enter the maximum packet size (Maximum Transfer Unit, MTU) in bytes that is allowed for the GRE connection between the partners. Possible values are *1* to *8192*. The default value is *1500*.
Use key	Enable the key input for the GRE connection, which makes it possible to distinguish between several parallel GRE connections between two GRE partners (see RFC 1701). The key is activated with *Enable*. The function is disabled by default.
Key Value	Only if **Use Key** is enabled. Enter the GRE connection key. Possible values are *0* to *2147483647*. The default value is *0*.

Chapter 17 Firewall

The Stateful Inspection Firewall (SIF) provided for **bintec** gateways is a powerful security feature.

The SIF with dynamic packet filtering has a decisive advantage over static packet filtering: The decision whether or not to send a packet cannot be made solely on the basis of source and destination addresses or ports but also using dynamic packet filtering based on the state of the connection to a partner.

This means packets that belong to an already active connection can also be forwarded. The SIF also accepts packets that belong to an "affiliated connection". The negotiation of an FTP connection takes place over port 21, for example, but the actual data exchange can take place over a completely different port.

SIF and other security features

bintec's Stateful Inspection Firewall fits into the existing security architecture of **bintec** device very well due to its simple configuration. The configuration work for the SIF is comparatively straightforward with systems like Network Address Translation (NAT) and IP Access Lists (IPAL).

As SIF, NAT and IPAL are active in the system simultaneously, attention must be given to possible interaction: If any packet is rejected by one of the security instances, this is done immediately. This is irrelevant whether another instance would accept it or not. Your need for security features should therefore be accurately analysed.

The essential difference between SIF and NAT/IPAL is that the rules for the SIF are generally applied globally, i.e. not restricted to one interface.

In principle, the same filter criteria are applied to the data traffic as those used in NAT and IPAL:

- Source and destination address of the packet (with an associated netmask)
- Service (preconfigured, e.g. Echo, FTP, HTTP)
- Protocol
- Port number(s)

To illustrate the differences in packet filtering, a list of the individual security instances and their method of operation is given below:

NAT

One of the basic functions of NAT is the translation of the local IP addresses of your LAN into the global IP addresses you are assigned by your ISP and vice versa. All connections initiated externally are first blocked, i.e. every packet your device cannot assign to an existing connection is rejected. This means that a connection can only be set up from inside to outside. Without explicit permission, NAT rejects every access from the WAN to the LAN.

IP Access Lists

Here packets are permitted or rejected exclusively on the basis of the criteria listed above, i.e. the state of the connection is not considered (except where **Services** = *tcp*).

SIF

The SIF sorts out all packets that are not explicitly or implicitly allowed. The result can be a "deny", in which case no error message is sent to the sender of the rejected packet, or a "reject", where the sender is informed of the packet rejection.

The incoming packets are processed as follows:

- The SIF first checks if an incoming packet can be assigned to an existing connection. If so, it is forwarded. If the packet cannot be assigned to an existing connection, a check is made to see if a suitable connection is expected (e.g. as affiliated connection of an existing connection). If so, the packet is also accepted.
- If the packet cannot be assigned to any existing or expected connection, the SIF filter rules are applied: If a deny rule matches the packet, the packet is rejected without sending an error message to the sender of the packet; if a reject rule matches, the packet is rejected and an ICMP Host Unreachable message sent to the sender of the packet. The packet is only forwarded if an accept rule matches.
- All packets without matching rules are rejected without sending an error message to the sender when all the existing rules have been checked (=default behaviour).

17.1 Policies

17.1.1 Filter Rules

The default behavior with **Action** = `Access` consists of two implicit filter rules: If an incoming packet can be assigned to an existing connection and if a suitable connection is expected (e.g. such as an affiliated connection of an existing connection), the packet is allowed.

The sequence of filter rules in the list is relevant: The filter rules are applied to each packet in succession until a rule matches. If overlapping occurs, i.e. more than one filter rule matches a packet, only the first rule is executed. This means that if the first rule denies a packet, whereas a later rule allows it, the packet is rejected. A deny rule also has no effect if a relevant packet has previously been allowed by another filter rule.

In the **Firewall** -> **Policies** -> **Filter Rules** menu, a list of all configured filter rules is shown.

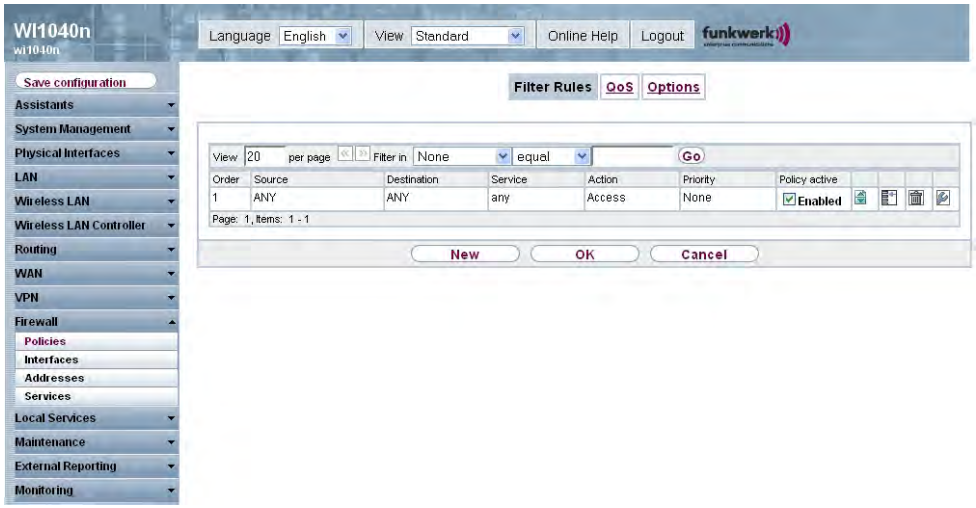


Fig. 124: **Firewall** -> **Policies** -> **Filter Rules**

You can use the button to insert another policy above the list entry. The configuration menu for creating a new policy opens.

You can use the button to move the list entry. A dialog box opens, in which you can select the position to which the policy is to be moved.

Moreover, the overview provides the option to show the firewall rules of the underlying settings made in the **System Management** -> **Administrative Access** -> **Access** menu. To do this, enable the **Show administrative access rules** option.

17.1.1.1 New

Choose the **New** button to set up new parameters.

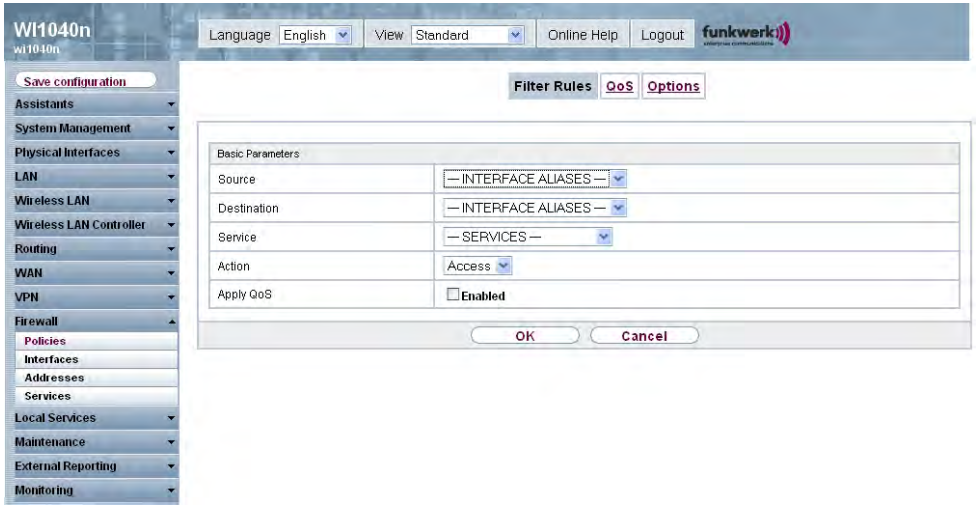


Fig. 125: **Firewall** -> **Policies** -> **Filter Rules** -> **New**

The **Firewall** -> **Policies** -> **Filter Rules** -> **New** menu consists of the following fields:

Fields in the Policies Basic Parameters menu

Field	Description
Source	Select one of the preconfigured aliases for the source of the packet. The list includes all WAN-/LAN interfaces, interface groups (see **Firewall** -> **Interfaces** -> **Groups**), addresses (see **Firewall** -> **Addresses** -> **Address List**) and address groups (see **Firewall** -> **Addresses** -> **Groups**) for selection. The value *Any* means that neither the source interface nor the source address is checked.
Destination	Select one of the preconfigured aliases for the destination of the packet. The list includes all WAN-/LAN interfaces, interface groups (see **Firewall** -> **Interfaces** -> **Groups**), addresses (see **Firewall** -> **Addresses** -> **Address List**) and address groups (see **Firewall** -> **Addresses** -> **Groups**) for selection.

Field	Description
	The value *Any* means that neither the destination interface nor the destination address is checked.
Service	Select one of the preconfigured services to which the packet to be filtered must be assigned. The extensive range of services configured ex works includes the following: • *FTP* • *TELNET* • *SMTP* • *DNS* • *HTTP* • *NNTP* • *Internet* • *Netmeeting* Other services are set up in **Firewall** -> **Services** -> **Service List**. In addition, the service groups configured in **Firewall** -> **Services** -> **Groups** can be selected.
Action	Select the action to be applied to a filtered packet. Possible values: • *Access* (default value): The packets are forwarded on the basis of the entries. • *Deny* : The packets are rejected. • *Reject* : The packets are rejected. An error message is issued to the sender of the packet.
Apply QoS	Only for **Action** = *Access* Select whether you want to enable QoS for this policy with the priority selected in **Data Traffic Priority** The function is activated with *Enabled*. The option is deactivated by default.

Field	Description
	If QoS is not activated for this policy, bear in mind that the data cannot be prioritised on the sender side either. A policy for which QoS has been enabled is also set for the firewall. Make sure therefore that data traffic that has not been expressly authorised if blocked by the firewall!
Priority	Only for **Apply QoS** = *enabled* Select the priority with which the data specified by the policy is handled on the send side. Possible values: • *None* (default value): No priority. • *Low Latency*: Low Latency Transmission (LTT), i.e. handling of data with the lowest possible latency, e.g. suitable for VoIP data. • *High* • *Medium* • *Low*

17.1.2 QoS

More and more applications need increasingly larger bandwidths, which are not always available. Quality of Service (QoS) makes it possible to distribute the available bandwidths effectively and intelligently. Certain applications can be given preference and bandwidth reserved for them.

In the **Firewall** -> **Policies** -> **QoS** menu, a list of all QoS rules is shown.

17.1.2.1 New

Choose the **New** button to set up new QoS rules.

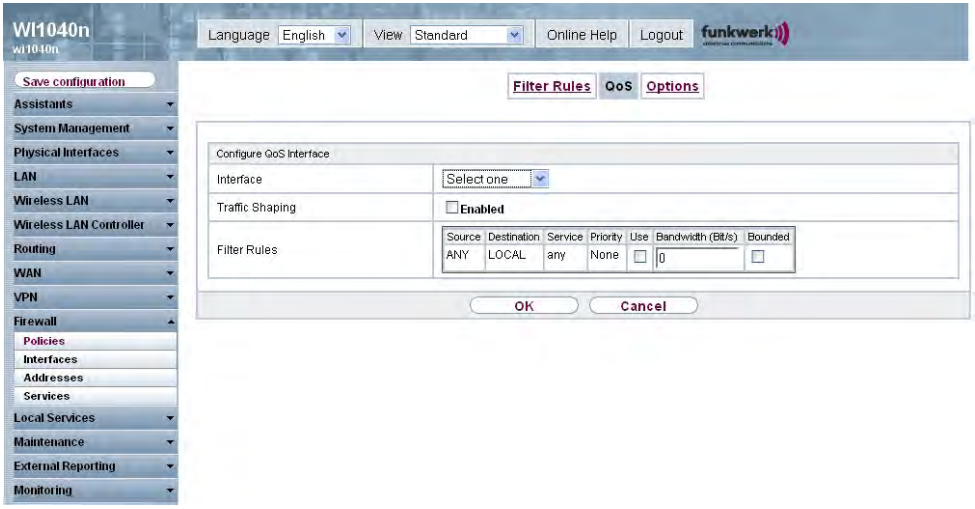


Fig. 126: **Firewall** -> **Policies** -> **QoS** -> **New**

The **Firewall** -> **Policies** -> **QoS** -> **New** menu consists of the following fields:

Fields in the QoS Configure QoS Interface menu

Field	Description
Interface	Select the interface on which bandwidth management is to be carried out.
Traffic Shaping	Select whether you want to activate bandwidth management for the selected interface. The function is activated with *Enabled*. The function is disabled by default.
Specify bandwidth	Only for **Traffic Shaping** = *Enabled*. Enter the maximum available bandwidth in kbps for the selected interface.
Filter Rules	This field contains a list of all configured firewall policies for which QoS was enabled (**Apply QoS** = *Enabled*). The following options are available for each list entry: • **Use**: Select whether this entry should be assigned to the QoS interface. The option is deactivated by default. • **Bandwidth**: Enter the maximum available bandwidth in Bps

Field	Description
	for the service specified under **Services**. *0* is entered by default. • **Fixed**: Select whether the bandwidth defined in **Bandwidth** can be exceeded in the longer term. By activating this field, you specify that it cannot be exceeded. If the option is deactivated, the bandwidth can be exceeded and the excess data rate is handled in accordance with the priority defined in the firewall policy. The option is deactivated by default.

17.1.3 Options

In this menu, you can disable or enable the firewall and can log its activities. In addition, you can define after how many seconds of inactivity a session shall be ended.

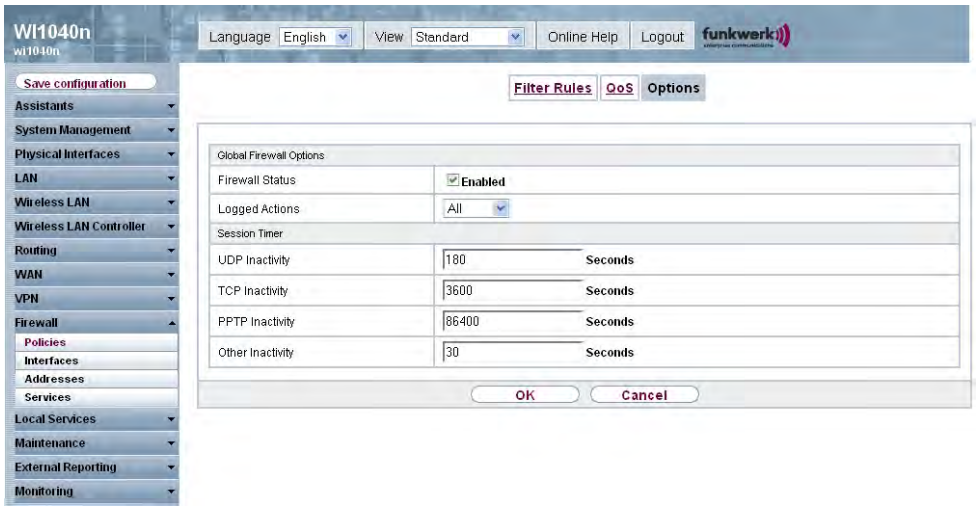


Fig. 127: **Firewall** -> **Policies** -> **Options**

The **Firewall** -> **Policies** -> **Options** menu consists of the following fields:

Fields in the Options Global Firewall Options menu

Field	Description
Firewall Status	Enable or disable the firewall function. The function is activated with *Enabled*. The function is enabled by default.

Field	Description
Logged Actions	Select the firewall syslog level. The messages are output together with messages from other subsystems. Possible values: • *All* (default value): All firewall activities are displayed. • *Deny* : Only reject and deny events are shown, see "Action". • *Accept* : Only accept events are shown. • *None*: Syslog messages are not generated.

Fields in the Options Session Timer menu

Field	Description
UDP Inactivity	Enter the inactivity time after which a UDP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *180*.
TCP Inactivity	Enter the inactivity time after which a TCP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *3600*.
PPTP Inactivity	Enter the inactivity time after which a PPTP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *86400*.
Other Inactivity	Enter the inactivity time after which a session of another type is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *30*.

17.2 Interfaces

17.2.1 Groups

In the **Firewall** -> **Interfaces** -> **Groups** menu, a list of all configured interface groups is shown.

You can group together the interfaces of your device. This makes it easier to configure firewall rules.

17.2.1.1 New

Choose the **New** button to set up new interface groups.

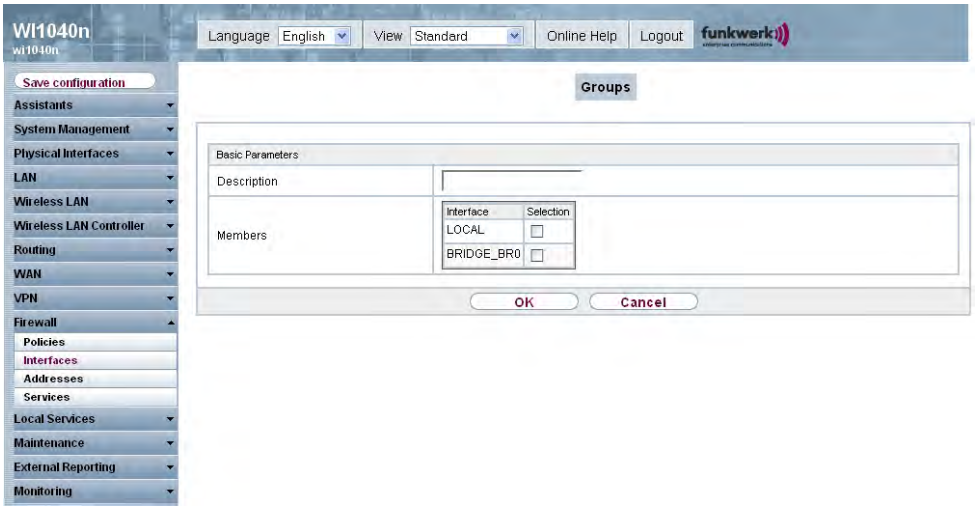


Fig. 128: **Firewall** -> **Interfaces** ->**Groups** -> **New**

The **Firewall** -> **Interfaces** -> **Groups** -> **New** menu consists of the following fields:

Fields in the Groups Basic Parameters menu

Field	Description
Description	Enter the desired description of the interface group.
Members	Select the members of the group from the available interfaces. To do this, activate the field in the **Members** column.

17.3 Addresses

17.3.1 Address List

In the **Firewall** -> **Addresses** -> **Address List** menu, a list of all configured addresses is shown.

17.3.1.1 New

Choose the **New** button to set up new addresses.

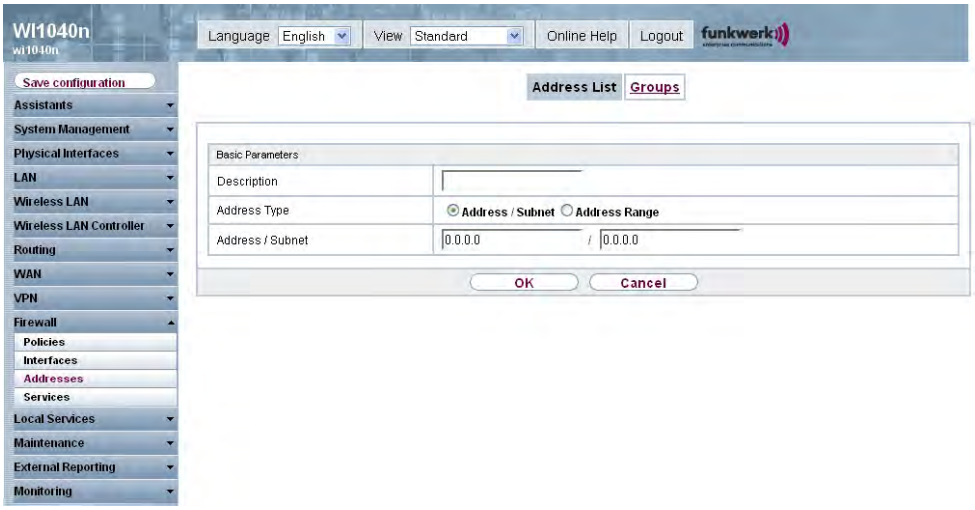


Fig. 129: **Firewall** -> **Addresses** -> **Address List** -> **New**

The **Firewall** -> **Addresses** -> **Address List** -> **New** menu consists of the following fields:

Fields in the Address List Basic Parameters menu

Field	Description
Description	Enter the desired description of the address.
Address Type	Select the type of address you want to specify. Possible values: • `Address / Subnet` (default value): Enter an IP address with subnet mask.

Field	Description
	• *Address Range*: Enter an IP address range with a start and end address.
Address / Subnet	Only if **Address Type** = *Address / Subnet* Enter the IP address of the host or a network address and the related netmask. The default value is *0.0.0.0*.
Address Range	Only if **Address Type** = *Address Range* Enter the start and end IP address of the range.

17.3.2 Groups

In the **Firewall** -> **Addresses** -> **Groups** menu, a list of all configured address groups is shown.

You can group together addresses. This makes it easier to configure firewall rules.

17.3.2.1 New

Choose the **New** button to set up new address groups.

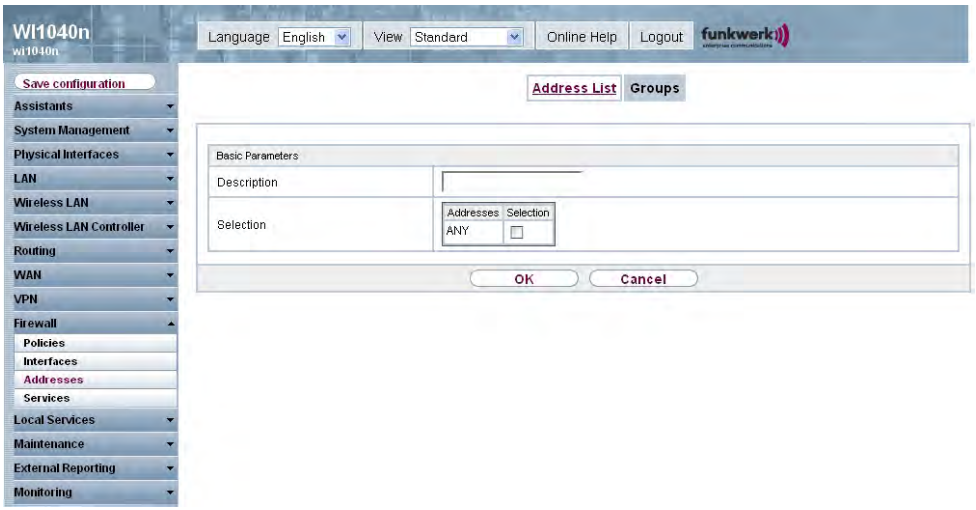


Fig. 130: **Firewall** -> **Addresses** -> **Groups** -> **New**

The **Firewall** -> **Addresses** -> **Groups** -> **New** menu consists of the following fields:

Fields in the Groups Basic Parameters menu

Field	Description
Description	Enter the desired description of the address group.
Selection	Select the members of the group from the available **Addresses**. To do this, enable the field in the **Selection** column.

17.4 Services

17.4.1 Service List

In the **Firewall** -> **Services** -> **Service List** menu, a list of all available services is shown.

17.4.1.1 New

Choose the **New** button to set up new services.

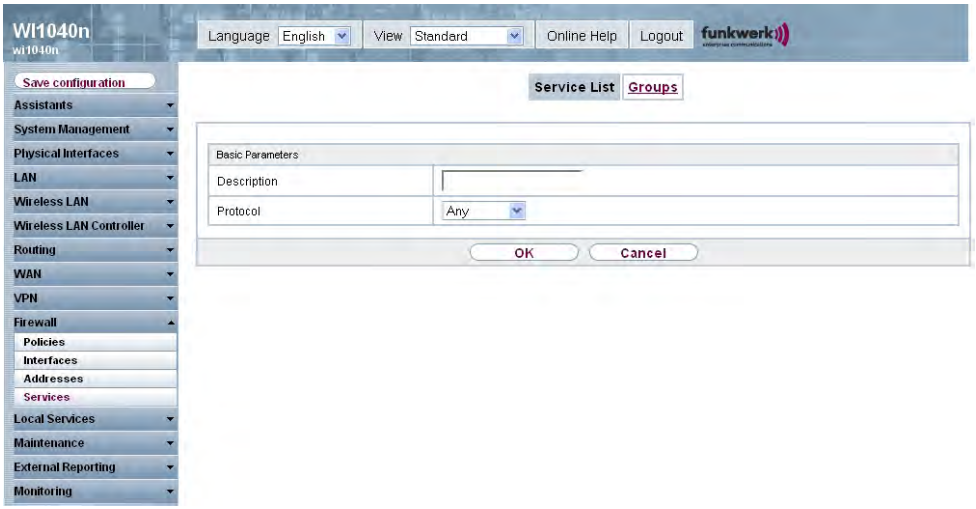


Fig. 131: **Firewall** -> **Services** -> **Service List** -> **New**

The **Firewall** -> **Services** -> **Service List** -> **New** menu consists of the following fields:

Fields in the Service List Basic Parameters menu

Field	Description
Description	Enter an alias for the service you want to configure.
Protocol	Select the protocol on which the service is to be based. The most important protocols are available for selection.
Destination Port Range	Only if **Protocol** = *TCP* , *UDP/TCP* or *UDP* In the first field, enter the destination port via which the service is to run. If a port number range is specified, in the second field enter the last port of the port range. By default the field does not contain an entry. If a value is displayed, this means that the previously specified port number is verified. If a port range is to be checked, enter the upper limit here. Possible values are *1* to *65535*.
Source Port Range	Only if **Protocol** = *TCP* , *UDP/TCP* or *UDP* In the first field, enter the source port to be checked, if applicable. If a port number range is specified, in the second field enter the last port of the port range. By default the field does not contain an entry. If a value is displayed, this means that the previously specified port number is verified. If a port range is to be checked, enter the upper limit here. Possible values are *1* to *65535*.
Type	Only if **Protocol** = *ICMP* The **Type** field shows the class of ICMP messages, the **Code** field specifies the type of message in greater detail. Possible values: • *Any* (default value) • *Echo Replay* • *Destination Unreachable* • *Source Quench* • *Redirect*

Field	Description
	• *Echo* • *Time Exceeded* • *Parameter Problem* • *Timestamp* • *Timestamp Reply* • *Information Request* • *Information Reply* • *Address Mask Request* • *Address Mask Reply*
Code	ICMP code options can only be selected if **Type** = *Destination Unreachable*. Possible values: • *Any* (default value) • *Net Unreachable* • *Host Unreachable* • *Protocol Unreachable* • *Port Unreachable* • *Fragmentation Needed* • *Communication with Destination Network is Administratively Prohibited* • *Communication with Destination Host is Administratively Prohibited*

17.4.2 Groups

In the **Firewall** -> **Services** -> **Groups** menu, a list of all configured service groups is shown.

You can group together services. This makes it easier to configure firewall rules.

17.4.2.1 New

Choose the **New** button to set up new service groups.

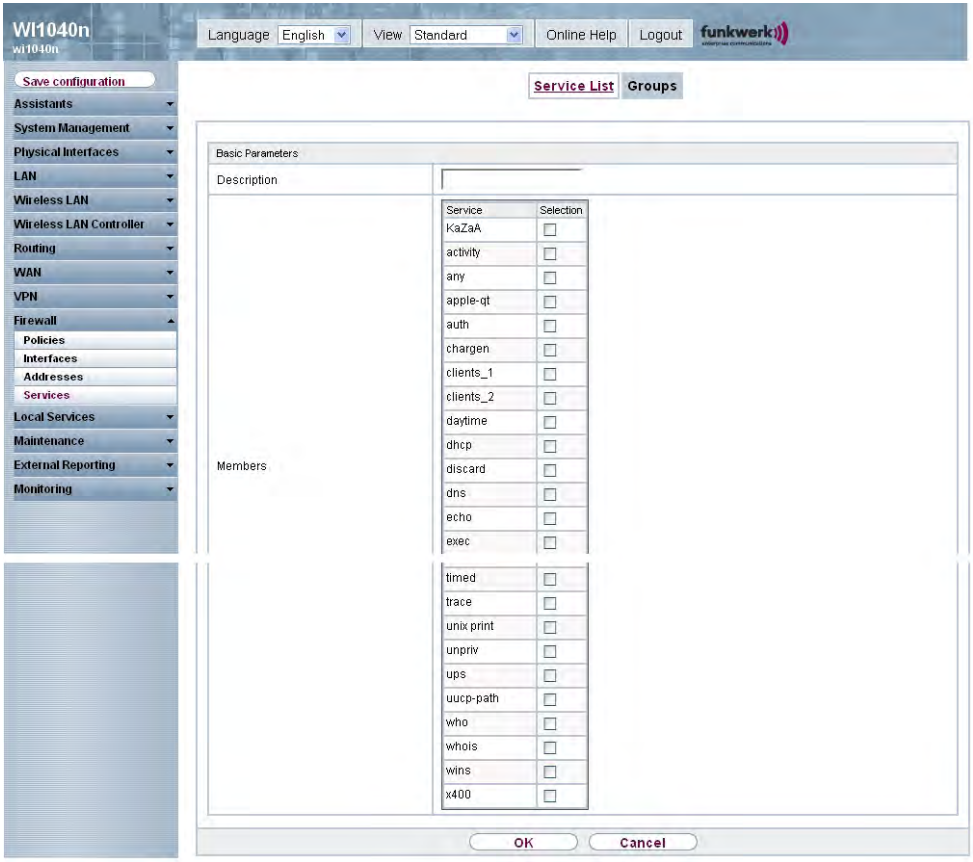


Fig. 132: **Firewall** -> **Services** ->**Groups**-> **New**

The **Firewall** -> **Services**-> **Groups** -> **New** menu consists of the following fields:

Fields in the Groups Basic Parameters menu

Field	Description
Description	Enter the desired description of the service group.
Members	Select the members of the group from the available service aliases. To do this, activate the field in the **Members** column.

Chapter 18 Local Services

This menu offers services for the following application areas:

- Name resolution (DNS)
- Locating of dynamic IP addresses using a DynDNS provider
- Configuration of gateway as a DHCP server (assignment of IP addresses)
- Access restriction on the Internet (web filter)
- Assignment of incoming and outgoing data and voice calls to authorised users (CAPI server)
- Automation of tasks according to schedule (scheduling)
- Alive checks for hosts or interfaces, ping tests
- User LAN protection (theft protection)
- Realtime video/audio conferences (Messenger services, universal plug & play)
- Provision of public Internet accesses (hotspot).

18.1 DNS

Each device in a TCP/IP network is usually located by its IP address. Because host names are often used in networks to reach different devices, it is necessary for the associated IP address to be known. This task can be performed by a DNS server, which resolves the host names into IP addresses. Alternatively, name resolution can also take place over the HOSTS file, which is available on all PCs.

Your device offers the following options for name resolution:

- DNS Proxy, for forwarding DNS requests sent to your device to a suitable DNS server. This also includes specific forwarding of defined domains (Forwarded Domains).
- DNS cache, for saving the positive and negative results of DNS requests.
- Static entries (Static Hosts), for manually defining or preventing assignments of IP addresses to names.
- DNS monitoring, for providing an overview of DNS requests on your device.

Global Name Server

The IP addresses of global name servers that are queried if your device is unable to answer requests itself or by forwarding entries are entered in **Local Services** -> **DNS** -> **Global Settings** -> **Basic Parameters**.

For local applications, the IP address of your device or the general loopback address (127.0.0.1) can be entered as the global name server.

Your device can also receive the global name servers dynamically and transfer them dynamically if necessary.

Strategy for name resolution on your device

A DNS request is handled by your device as follows:

(1) If possible, the request is answered directly from the static or dynamic cache with IP address or negative response.

(2) Otherwise, if a suitable forwarding entry exists, the relevant DNS server is asked, depending on the configuration of the Internet or dialin connections, if necessary by setting up a WAN connection at extra cost. If the DNS server can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(3) Otherwise, if global name servers are entered, the primary DNS server then the secondary DNS server are asked. If the IP address of your device or the loopback address is entered for local applications, these are ignored here. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(4) Otherwise, if a suitable Internet or dialin connection is selected as the standard interface, the relevant DNS server is asked, depending on the configuration of the Internet or dialin connections, if necessary by setting up a WAN connection at extra cost. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(5) Otherwise, if overwriting the addresses of the global name servers is allowed (**DNS Server Configuration** = *Dynamic*), a connection is set up – in some cases at extra cost – that is configured to enable DNS server addresses to be requested from DNS servers (**DNS Negotiation** = *Enabled*), if this has not been attempted previously. If name server negotiation is successful, these are entered as global name servers and are therefore available for further requests.

(6) Otherwise the initial request is answered with a server error.

If one of the DNS servers answers with `non-existent domain`, the initial request is immediately answered accordingly and a corresponding negative entry is made in the DNS cache of your device.

18.1.1 Global Settings

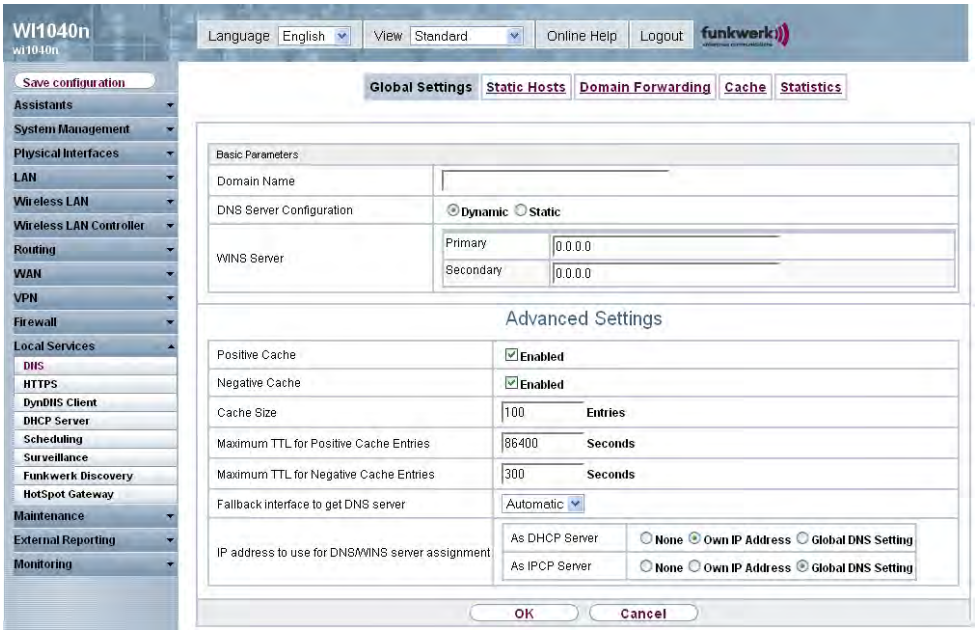


Fig. 133: **Local Services** -> **DNS** -> **Global Settings**

The menu **Local Services** -> **DNS** -> **Global Settings** consists of the following fields:

Fields in the Global Settings Basic Parameters menu

Field	Description
Domain Name	Enter the standard domain name of your device.
DNS Server Configuration	Select whether the addresses of the global name server on your device can be overwritten by transferred name server addresses. Possible values: • `Dynamic` (default value) The name server addresses can be automatically overwritten. • `Static`: The name server addresses are not overwritten.
DNS Server Primary	Only for **DNS Server Configuration** = `Static` Enter the IP address of the first and, if necessary, second global

Field	Description
Secondary	DNS server.
WINS Server Primary Secondary	Enter the IP address of the first and, if necessary, alternative global Windows Internet Name Server (=WINS) or NetBIOS Name Server (=NBNS).

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Positive Cache	Select whether the positive dynamic cache is to be activated, i.e. successfully resolved names and IP addresses are to be stored in the cache. The function is activated by choosing *Enabled*. The function is enabled by default.
Negative Cache	Select whether the negative dynamic cache is to be activated, i.e. whether queried names for which a DNS server has sent a negative response are stored as negative entries in the cache. The function is activated by choosing *Enabled*. The function is enabled by default.
Cache Size	Enter the maximum total number of static and dynamic entries. Once this value is reached, the dynamic entry not requested for the longest period of time is deleted when a new entry is added. If the **Cache Size** is reduced by the user, dynamic entries are deleted if necessary. Static entries are not deleted. **Cache Size** cannot be set to smaller than the current number of static entries. Possible values: *0* .. *1000* . The default value is *100*.
Maximum TTL for Positive Cache Entries	Enter the value to which the TTL is to be set for a positive dynamic DNS entry in the cache if its TTL *0* is or its TTL exceeds the value for **Maximum TTL for Positive Cache Entries**.

Field	Description
	The default value is *86400*.
Maximum TTL for Negative Cache Entries	Enter the value set to which the TTL is to be set in the case of a negative dynamic entry in the cache. The default value is *86400*.
Fallback interface to get DNS server	Only if **DNS Server Configuration** = *Dynamic*Select the interface to which a connection is set up for name server negotiation if other name resolution attempts were not successful. The default value is *Automatic* i.e. a one-time connection is set up to the first suitable connection partner configured in the system.
IP address to use for DNS/WINS server assignment	**As DHCP Server** Select which name server addresses are sent to the DHCP client if your device is used as DHCP server. Possible values: • *None*: No name server address is sent. • *Own IP Address* (default value): The address of your device is transferred as the name server address. • *Global DNS Setting*: The addresses of the global name servers entered on your device are sent. **As IPCP Server** Select which name server addresses are to be transmitted by your device in the event of dynamic server name negotiation if your device is used as the IPCP server for PPP connections. Possible values: • *None*: No name server address is sent. • *Own IP Address*: The address of your device is transferred as the name server address. • *Global DNS Setting* (default value): The addresses of the global name servers entered on your device are sent.

18.1.2 Static Hosts

In the **Local Services** -> **DNS** -> **Static Hosts** menu, a list of all configured static hosts is shown.

18.1.2.1 New

Choose the **New** button to set up new static hosts.

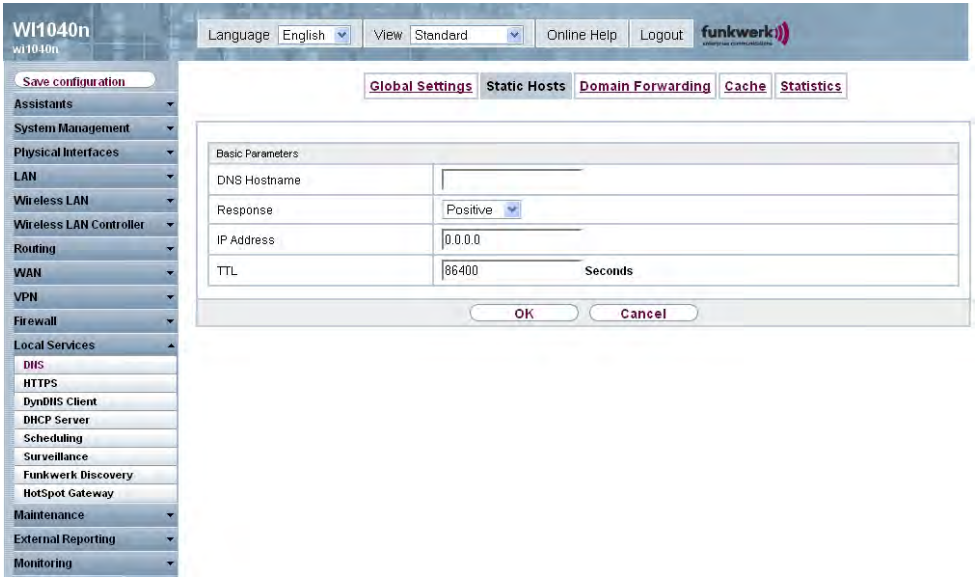


Fig. 134: **Local Services** -> **DNS** -> **Static Hosts** -> **New**

The **Local Services** -> **DNS** -> **Static Hosts** -> **New** menu consists of the following fields:

Fields in the Static Hosts Basic Parameters menu

Field	Description
DNS Hostname	Enter the host name to which the **IP Address** defined in this menu is to be assigned if a positive response is received to a DNS request. If a negative response is received to a DNS request, no address is specified. The entry can also start with the wildcard *, e.g. *.funkwerk.de. If a name is entered without a dot, this is completed with **<Name>.** after confirming with **OK** " " is added.

Field	Description
	Entries with spaces are not allowed.
Response	In this entry, select the type of response to DNS requests. Possible values: • *Negative* : A DNS request for **Name** is answered with a negative response. • *Positive* (default value): A DNS request for **Name** is answered with the associated **IP Address**. • *None*: A DNS request is ignored; no answer is given.
IP Address	Only if **Response** = *Positive*. Enter the IP address assigned to **Name**.
TTL	Enter the the time for which the assignment of **Name** to **IP Address** is to be valid in seconds (only relevant if **Response** = *Positive*) that is transferred to requesting hosts. The default value is *86400* (= 24 h).

18.1.3 Domain Forwarding

In the **Local Services** -> **DNS** -> **Domain Forwarding** menu, a list of all configured forwarding for defined domains is shown.

18.1.3.1 New

Choose the **New** button to set up new forwardings.

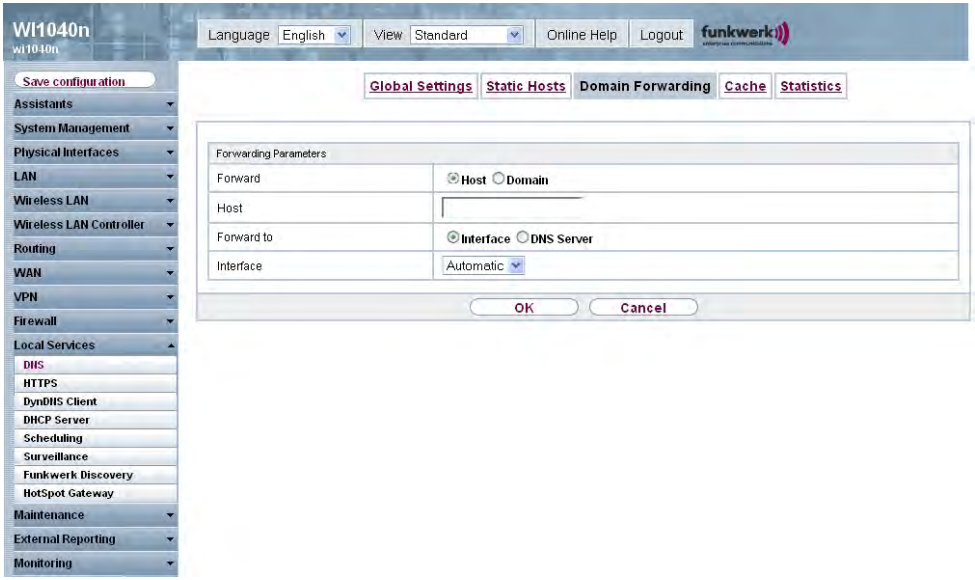


Fig. 135: **Local Services** -> **DNS** -> **Domain Forwarding** -> **New**

The **Local Services** -> **DNS** -> **Domain Forwarding** -> **New** menu consists of the following fields:

Fields in the Domain Forwarding Forwarding Parameters menu

Field	Description
Forwarding	Select whether a host or domain is to be forwarded. Possible values: • `Host` (default value) • `Domain`
Host	Only for **Forward** = `Host` Enter the name of the host to be forwarded. The entry can also start with the wildcard *, e.g. *.funkwerk.com. If a name is entered without a full stop, once you confirm with **OK** " **<Default Domain>.** " " is added.
Domain	Only for **Forward** = `Domain` Enter the name of the domain to be forwarded. The entry can also start with the wildcard *, e.g. *.funkwerk.com.

Field	Description
	If a name is entered without a full stop, once you confirm with **OK** " **<Default Domain>.** " " is added.
Forward to	Select the forwarding destination requests to the name defined in **Host** or **Domain**. Possible values: • *Interface* (default setting) The request is forwarded to the defined **Interface**. • *DNS Server*: The request is forwarded to the defined **DNS server**.
Interface	Only for **Forward to** = *Interface* Select the interface via which the requests for the defined **Domain** are to be received and forwarded to the DNS server.
DNS Server	Only for **Forward to** = *DNS server* Enter the IP address of the primary and secondary DNS server.

18.1.4 Cache

In the **Local Services** -> **DNS** -> **Cache** menu, a list of all available cache entries is shown.

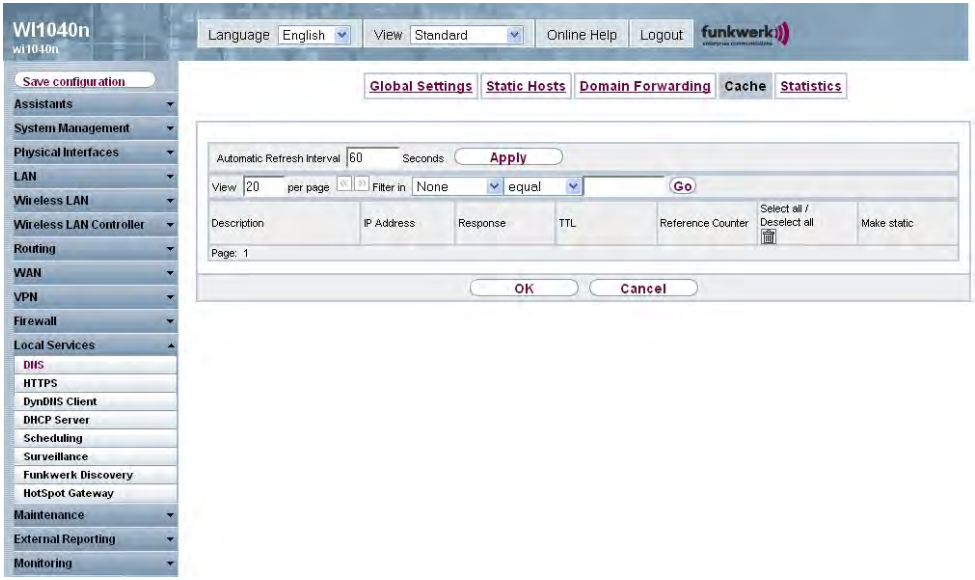


Fig. 136: **Local Services** -> **DNS** -> **Cache**

You can select individual entries using the checkbox in the corresponding line, or select them all using the **Select All** button.

A dynamic entry can be converted to a static entry by marking the entry and confirming with **Set to Static**. This entry then disappears from the list and is included in the list in the **Static Hosts** menu. The TTL is transferred in this operation.

18.1.5 Statistics

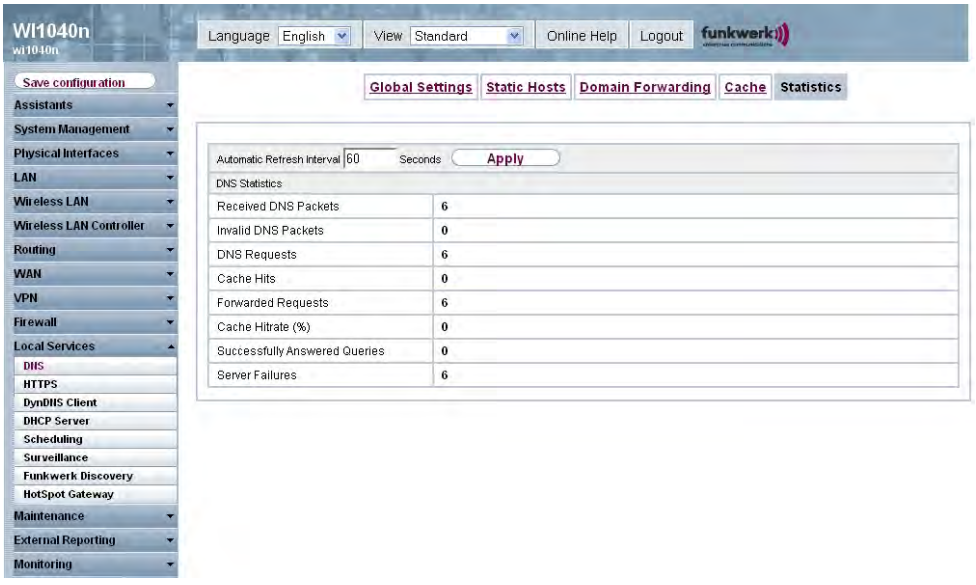


Fig. 137: **Local Services** -> **DNS** -> **Statistics**

In the menu **Local Services** -> **DNS** -> **Statistics**, the following statistical values are shown:

Fields in the Statistics DNS Statistics menu

Field	Description
Received DNS Packets	Shows the number of received DNS packets addressed direct to your device, including the response packets for forwarded requests.
Invalid DNS Packets	Shows the number of invalid DNS packets received and addressed direct to your device.
DNS Requests	Shows the number of valid DNS requests received and addressed direct to your device.
Cache Hits	Shows the number of requests that were answered with static or dynamic entries from the cache.
Forwarded Requests	Shows the number of requests forwarded to other name servers.
Cache Hitrate (%)	Displays the number of **Cache Hits** per **DNS Request** in %.
Successfully Answered Queries	Shows the number of successfully answered requests (positive and negative).

Field	Description
Server Failures	Shows the number of requests that were not answered by any name server (either positively or negatively).

18.2 HTTPS

You can operate the user interface of your device from any PC with an up-to-date Web browser via an HTTPS connection.

HTTPS (HyperText Transfer Protocol Secure) is the procedure used to establish an encrypted and authenticated connection by SSL between the browser used for configuration and the device.

18.2.1 HTTPS server

In the **Local Services** -> **HTTPS** -> **HTTPS Server** menu you configure the parameters of the secure configuration connection over HTTPS.

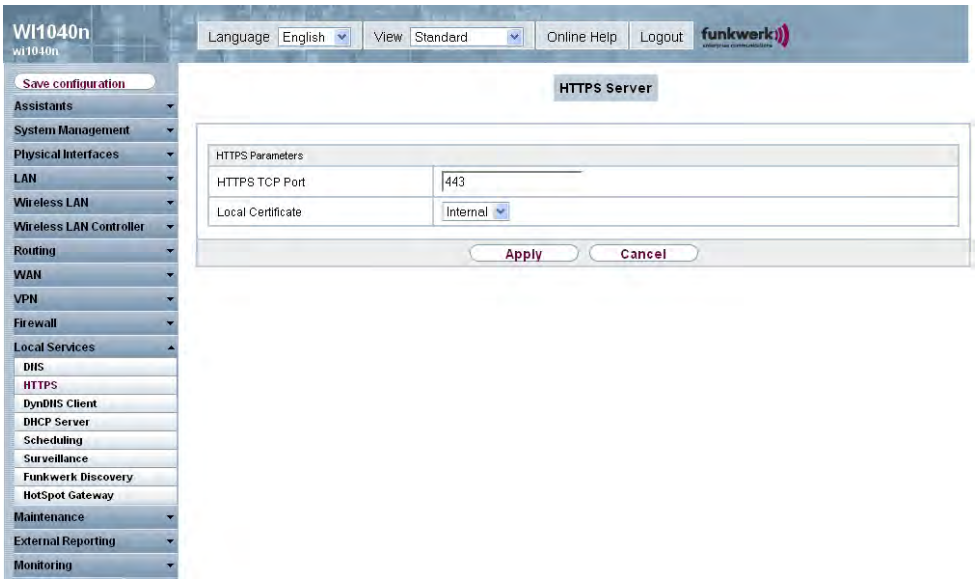


Fig. 138: **Local Services** -> **HTTPS** -> **HTTPS Server**

The **Local Services** -> **HTTPS** -> **HTTPS Server** menu consists of the following fields:

Fields in the HTTPS Server HTTPS Parameters menu

Field	Description
HTTPS TCP Port	Enter the port via which the HTTPS connection is to be established. Possible values are *0* to *65535*. The default value is *443*.
Local Certificate	Select a certificate that you want to use for the HTTPS connection. Possible values: • *Internal* (default value): Select this option if you want to use the certificate built into the device. • *<Certificate name>*: Select the entered certificate under **System Management** -> **Certificates** -> **Certificate List** .

18.3 DynDNS Client

The use of dynamic IP addresses has the disadvantage that a host in the network can no longer be found once its IP address has changed. DynDNS ensures that your device can still be reached after a change to the IP address.

The following configuration steps are necessary:

- Registration of a host name at a DynDNS provider
- Configuration of your device

Registration

The registration of a host name means that you define an individual user name for the DynDNS service, e.g. *dyn_client*. The service providers offer various domain names for this, so that a unique host name results for your device , e.g. *dyn_client.provider.com*. The DynDNS provider relieves you of the task of answering all DNS requests concerning the host *dyn_client.provider.com* with the dynamic IP address of your device.

To ensure that the provider always knows the current IP address of your device, your device contacts the provider when setting up a new connection and propagates its present IP address.

18.3.1 DynDNS Update

In the **Local Services** -> **DynDNS Client** -> **DynDNS Update** menu, a list of all configured DynDNS registrations is shown that are to be updated.

18.3.1.1 New

Choose the **New** button to set up further DynDNS registrations to be updated.

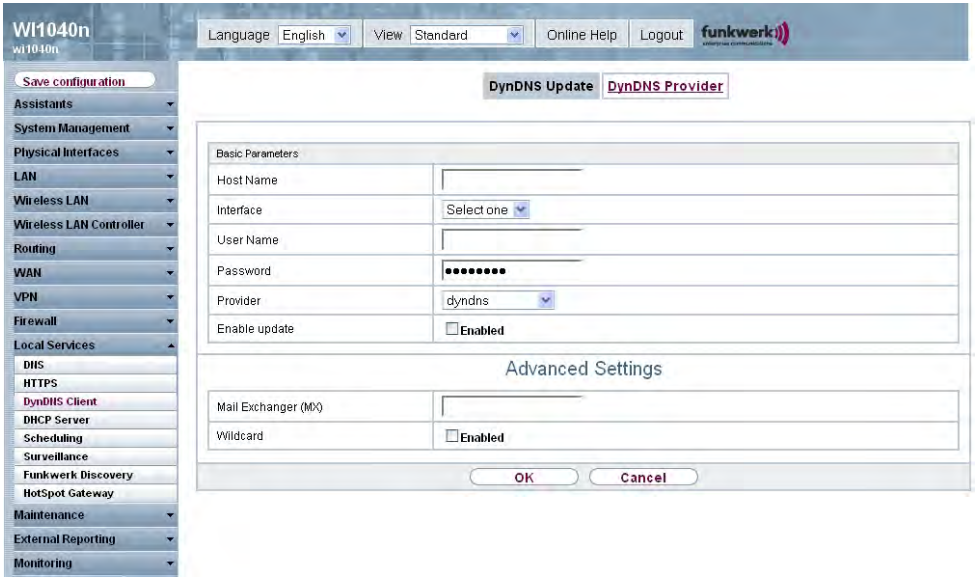


Fig. 139: **Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**

The **Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New** menu consists of the following fields:

Fields in the DynDNS Update Basic Parameters menu

Field	Description
Host Name	Enter the complete host name as registered with the DynDNS provider.
Interface	Select the WAN interface whose IP address is to be propagated over the DynDNS service (e.g. the interface of the Internet Service Provider).
User Name	Enter the user name as registered with the DynDNS provider.

Field	Description
Password	Enter the password as registered with the DynDNS provider.
Provider	Select the DynDNS provider with which the above data is registered. A choice of DynDNS providers is already available in the unconfigured state and their protocols are supported. Other DynDNS providers can be configured in the **Local Services** -> **DynDNS Client**-> **DynDNS Providers** menu. The default value is *DynDNS* .
Enable update	Select whether the DynDNS entry configured here is to be activated. The function is activated by choosing *Enabled*. The function is disabled by default.

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Mail Exchanger (MX)	Enter the full host name of a mail server to which e-mails are to be forwarded if the host currently configured is not to receive mail. Ask your provider about this forwarding service and make sure e-mails can be received from the host entered as MX.
Wildcard	Select whether the forwarding of all subdomains of the **Host Name** are to be enabled for the current IP address of the **Interface** (advanced name resolution). The function is activated by choosing *Enabled*. The function is disabled by default.

18.3.2 DynDNS Provider

In the **Local Services** -> **DynDNS Client** -> **DynDNS Provider** menu, a list of all configured DynDNS providers is shown.

18.3.2.1 New

Choose the **New** button to set up new DynDNS providers.

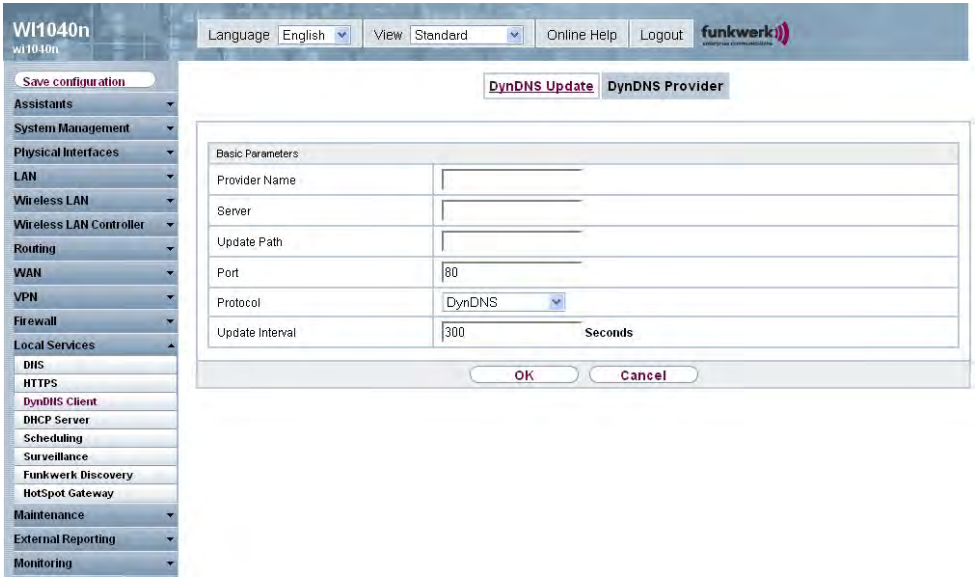


Fig. 140: **Local Services** -> **DynDNS Client** -> **DynDNS Provider** -> **New**

The **Local Services** -> **DynDNS Client** -> **DynDNS Provider** -> **New** menu consists of the following fields:

Fields in the DynDNS Provider Basic Parameters menu

Field	Description
Provider Name	Enter a name for this entry.
Server	Enter the host name or IP address of the server on which the provider's DynDNS service runs.
Update Path	Enter enter the path on the provider's server that contains the script for managing the IP address of your device. Ask your provider for the path to be used.
Port	Enter the port at which your device is to reach your provider's server. Ask your provider for the relevant port.

Field	Description
	The default value is *80*.
Protocol	Select one of the protocols implemented. Possible values: • *DynDNS* (default value) • *Static DynDNS* • *ODS* • *HN* • *DYNS* • *GnuDIP-HTML* • *GnuDIP-TCP* • *Custom DynDNS* • dnsexit
Update Interval	Enter the minimum time (in seconds) that your device must wait before it is allowed to propagate its current IP address to the DynDNS provider again. The default value is *300* seconds.

18.4 DHCP Server

You can configure your device as a DHCP (Dynamic Host Configuration Protocol) server.

Your device and each PC in your LAN requires its own IP address. One option for allocating IP addresses in your LAN is the Dynamic Host Configuration Protocol (DHCP). If you configure your device as a DHCP server, the device automatically assigns IP addresses to requesting PCs in the LAN from a predefined IP address pool. A PC sends out an ARP request and in turn receives its IP address assigned by your device. You therefore do not need to allocate fixed IP addresses to PCs, which reduces the amount of configuration work in your network. To do this, you set up a pool of IP addresses, from which your device assigns IP addresses to hosts in the LAN for a defined period of time. A DHCP server also transfers the addresses of the domain name server entered statically or by PPP negotiation (DNS), NetBIOS name server (WINS) and default gateway.

18.4.1 DHCP Pool

To activate your device as a DHCP server, you must first define IP address pools from which the IP addresses are distributed to the requesting clients.

In the **Local Services** -> **DHCP Server** -> **DHCP Pool** menu, a list of all configured IP address pools is shown.

In the list, for each entry, you have the possibility under **Pool** of enabling or disabling the configured DHCP pools.

18.4.1.1 New

Choose the **New** button to set up new IP address pools. Choose the icon to edit existing entries.

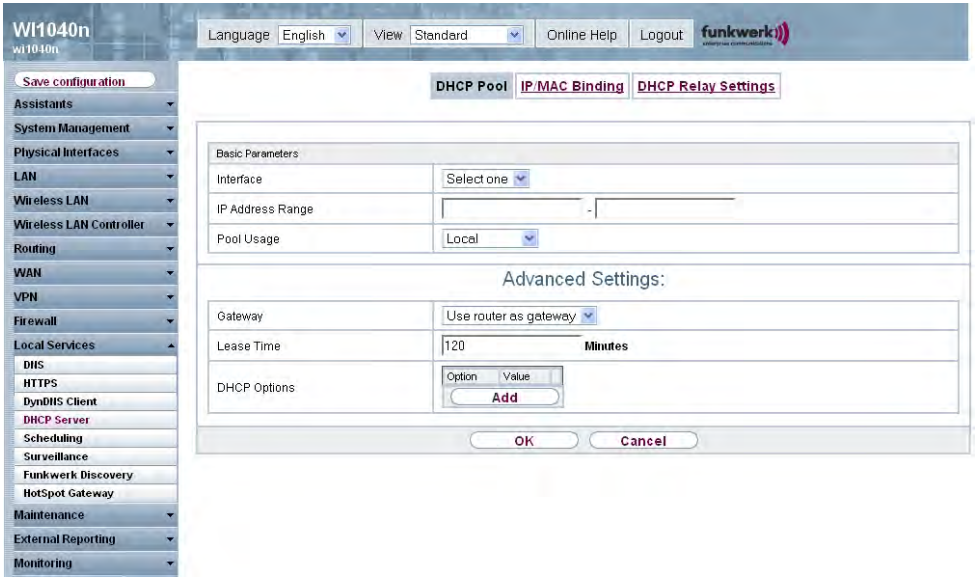


Fig. 141: **Local Services** -> **DHCP Server** -> **DHCP Pool** -> **New**

The **Local Services** -> **DHCP Server** ->**DHCP Pool** -> **New** menu consists of the following fields:

Fields in the DHCP Pool Basic Parameters menu

Field	Description
Interface	Select the interface over which the addresses defined in **IP Range** are to be assigned to DHCP clients.

Field	Description
	When a DHCP request is received over this **Interface**, one of the addresses from the address pool is assigned.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
Pool Usage	Specify whether the IP pool is used for DHCP requests in the same subnet or for DHCP requests that have been forwarded to your device from another subnet. In this case it is possible to define IP addresses from another network. Possible values: • *Local* (default value): The DHCP pool is only used for DHCP requests in the same subnet. • *Local/Relay*: The DHCP pool is used for DHCP requests in the same subnet and from other subnets. • *Relay*: The DHCP pool is only used for DHCP requests forwarded from other subnets.

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Gateway	Select which IP address is to be transferred to the DHCP client as gateway. Possible values: • *No gateway* (default value): No IP address is sent. • *Use router as gateway*: The IP address defined for the **Interface** is transferred. • *Specify*: Enter the corresponding IP address.
Lease Time	Enter the length of time (in minutes) for which an address from the pool is to be assigned to a host. After the **Lease Time (Minutes)** expires, the address can be re-assigned by the server. The default value is *120*.

Field	Description
DHCP Options	Specify which additional data is forwarded to the DHCP client. Possible values for **Option**: • *Time Server* (default value): Enter the IP address of the time server to be sent to the client. • *DNS Server*: Enter the IP address of the DNS server to be sent to the client. • *DNS Domain Name*: Enter the DNS domain to be sent to the client. • *WINS/NBNS Server*: Enter the IP address of the WINS/NBNS server to be sent to the client. • *WINS/NBT Node Type*: Enter the type of the WINS/NBT node to be sent to the client. • *TFTP Server*: Enter the IP address of the TFTP server to be sent to the client. Several entries are possible. Add new entries with the **Add** button.

18.4.2 IP/MAC Binding

In the **Local Services** -> **DHCP Server** -> **IP/MAC Binding** menu a list is shown of all clients that have received an IP address from your device via DHCP.

You can now allocate an IP address from a defined IP address pool to specific MAC addresses. You can do this by selecting the **Static Binding** option in the list to convert a list entry as a fixed binding, or you manually create a fixed IP/MAC binding by configuring this in the **New** sub-menu.

Note

You can only create new static IP/MAC bindings if IP address ranges have been configured in **Local Services** -> **DHCP Server** -> **DHCP Pool**.

18.4.2.1 New

Choose the **New** button to set up new IP/MAC bindings.

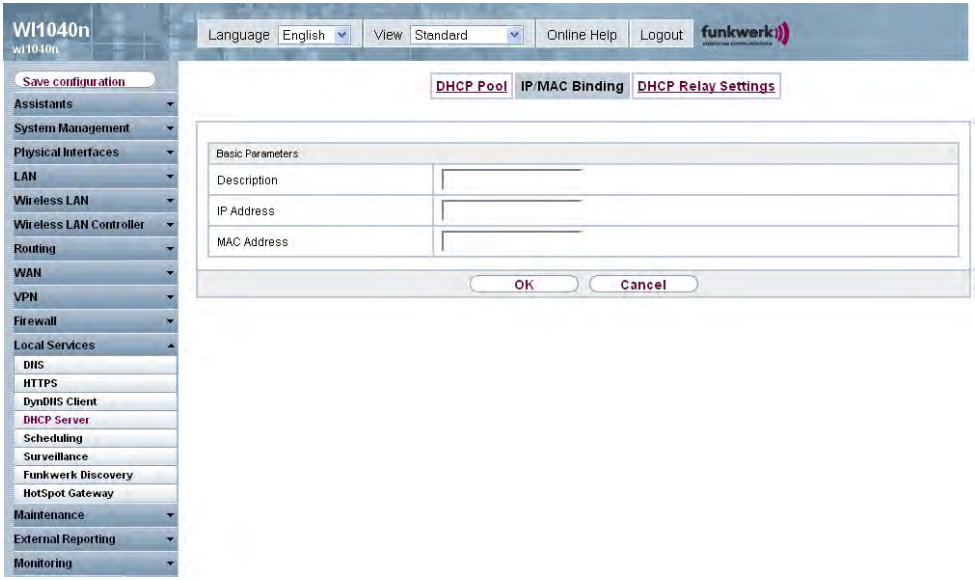


Fig. 142: **Local Services** -> **DHCP Server** -> **IP/MAC Binding** -> **New**

The **Local Services** -> **DHCP Server** ->**DHCP Binding** -> **New** menu consists of the following fields:

Fields in the IP/MAC Binding Basic Parameters menu

Field	Description
Description	Enter the name of the host to the **MAC Address** of which the **IP Address** is to be bound. A character string of up to 256 characters is possible.
IP Address	Enter the IP address to be assigned to the MAC address specified in **MAC Address**.
MAC Address	Enter the MAC address to which the IP address specified in **IP Address** is to be assigned.

18.4.3 DHCP Relay Settings

If your device for the local network does not distribute any IP addresses to the clients by DHCP, it can still forward the DHCP requests on behalf of the local network to a remote DHCP server. The DHCP server then assigns the your device an IP address from its pool, which in turn sends this to the client in the local network.

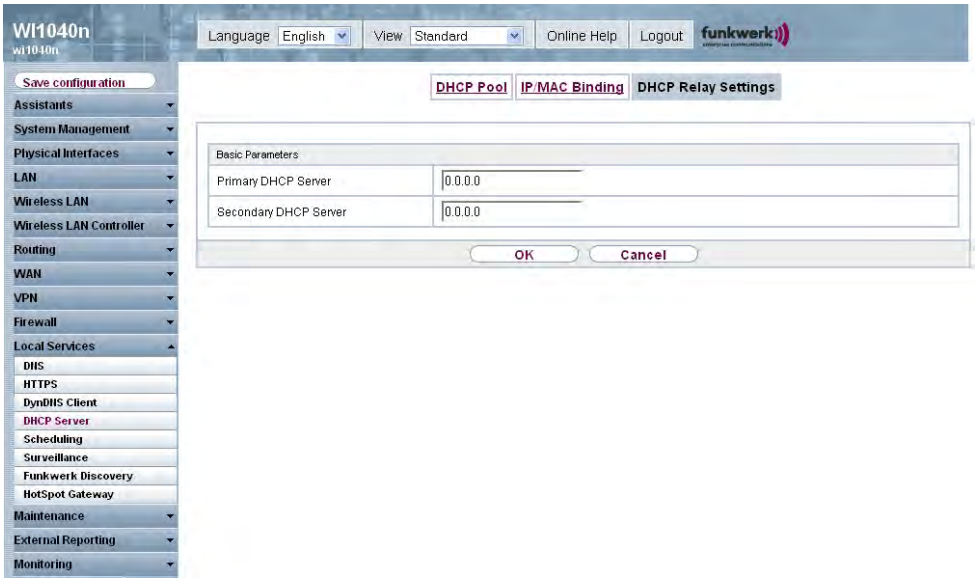


Fig. 143: **Local Services** -> **DHCP Server** -> **DHCP Relay Settings**

The **Local Services** -> **DHCP Server** -> **DHCP Relay Settings** menu consists of the following fields:

Fields in the DHCP Relay Settings Basic Parameters menu

Field	Description
Primary DHCP Server	Enter the IP address of a server to which BootP or DHCP requests are to be forwarded.
Secondary DHCP Server	Enter the IP address of an alternative BootP or DHCP server.

18.5 Scheduling

Your device has a event scheduler, which enables certain standard actions (activation or deactivation of interfaces) to be carried out on a time-dependent basis.

Note

To run the event scheduler, the date configured on your device must be 1.1.2000 or later.

18.5.1 Schedule

In the **Local Services** -> **Scheduling** -> **Time Schedule** menu, a list of all scheduled tasks is shown.

18.5.1.1 New

Choose the **New** button to set up new tasks.

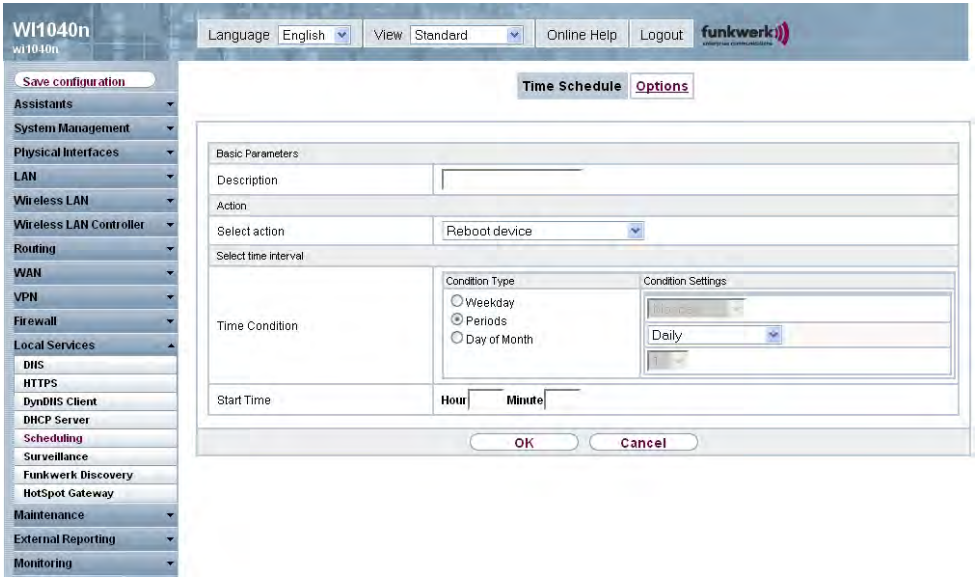


Fig. 144: **Local Services** -> **Scheduling** -> **Time Schedule** -> **New**

The **Local Services** -> **Scheduling** -> **Time Schedule**-> **New** menu consists of the following fields:

Fields in the Time Schedule Basic Parameters menu

Field	Description
Description	Enter the desired name for the scheduled task.

Fields in the Time Schedule Action menu

Field	Description
Select action	Select the desired action. Possible values:

Field	Description
	• *Reboot device* (default value): Your device is rebooted. • *Activate interface* : The interface defined in the **Select Interface** field is activated. • *Deactivate interface* : The interface defined in the **Select Interface** field is deactivated. • *Activate WLAN*: The WLAN interface defined in the **Select Interface** field is activated. • *Deactivate WLAN*: The WLAN interface defined in the **Select Interface** field is deactivated. • *Initiate 5 GHz WLAN Bandscan*: The wireless module selected in **Select Wireless Module** is scanned in the 5-GHz frequency band. During the scan, all wireless connections are interrupted. • *Trigger software update*: A software update is initiated. • *Trigger configuration backup*: The backup of the device configuration to a TFTP server is initiated.
Select radio	Only if **Select action** = *Initiate 5 GHz WLAN Bandscan* Select the wireless module to be used for the scan.
Select interface	Only if **Select action** = *Activate interface* or *Deactivate interface* or if **Select action** = *Activate WLAN* or *Deactivate WLAN* Select which interface is to be activated or deactivated.
Source Location	Only if **Select action** = *Trigger software update* Select the desired source. Possible values: • *Current software from Funkwerk server*: The latest software will be downloaded from the Funkwerk server. • *HTTP server*: The latest software will be downloaded from an HTTP server that you define in *Update URL*.
Update URL	Only if **Select action** = *Trigger software update* and

Field	Description
	Source = *HTTP Server* Enter the name of the HTTP server from which you wish to download a configuration file.
TFTP Server	Only if **Select action** = *Trigger configuration backup* Enter the IP address of the TFTP server to which you wish to transfer a configuration file.
TFTP File Name	Only if **Select action** = *Trigger configuration backup* Enter the name with which configuration file is to be transferred to the TFTP server.

Fields in the Time Schedule Select time interval menu

Field	Description
Time Condition	First select the type of time entry in **Condition Type**. Possible values: • *Weekday*: In **Condition Settings** , select a weekday. • *Periods* (default setting): In **Condition Settings** , select a particular period. • *Day of Month*: In **Condition Settings** , select a particular day of the month. Possible values for **Condition Settings** with **Condition Type** = *Weekday*: *Monday* (default value) ... *Sunday*. Possible values for **Condition Settings** with **Condition Type** = *Periods*: • *Daily*: The initiator becomes active daily (default value). • *Monday-Friday*: The initiator becomes active daily from Monday to Friday. • *Monday-Saturday* : The initiator becomes active daily from Monday to Saturday. • *Saturday - Sunday* : The initiator becomes active on Saturdays and Sundays.

Field	Description
	Possible values for **Condition Settings** with **Condition Type** = *Day of the month*: *1* ... *31*.
Start Time	Enter the time from which the initiator is to be activated. Activation is carried on the next scheduling interval. the default value of this interval is 55 seconds.
Stop Time	Not if **Select Action** = *Reboot device* Enter the time from which the initiator is to be deactivated. Deactivation is carried on the next scheduling interval. If you do not enter a **Stop Time** or set **Stop Time** = **Start Time**, the initiator is activated and deactivated after 10 seconds.

18.5.2 Options

In the **Local Services** -> **Scheduling** -> **Options** menu, you configure the schedule interval.

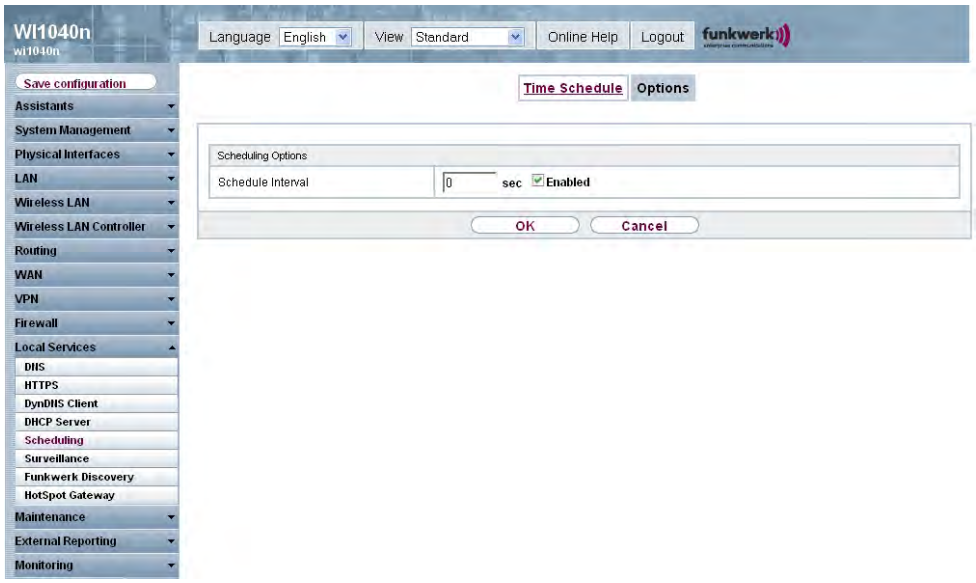


Fig. 145: **Local Services** -> **Scheduling** -> **Options**

The **Local Services** -> **Scheduling** -> **Options** menu consists of the following fields:

Fields in the Options Scheduling Options menu

Field	Description
Schedule Interval	Select whether the schedule interval is to be enabled for the interface. Enter the interval in seconds during which the system checks whether there are planned tasks. Possible values are *0* to *65535*. The value *300* is recommended (5 minute accuracy). Values lower than 60 are generally pointless and are an unnecessary use of system resources. The field is not activated by default.

18.6 Surveillance

In this menu, you can configure an automatic availability check for hosts or interfaces and automatic ping tests.

Note

This function cannot be configured on your device for connections that are authenticated via a RADIUS server.

18.6.1 Hosts

In the **Local Services** -> **Surveillance** -> **Hosts** menu, a list of all monitored hosts is shown.

18.6.1.1 Edit/New

Choose the icon to edit existing entries. Choose the **New** button to set up new surveillance tasks servers.

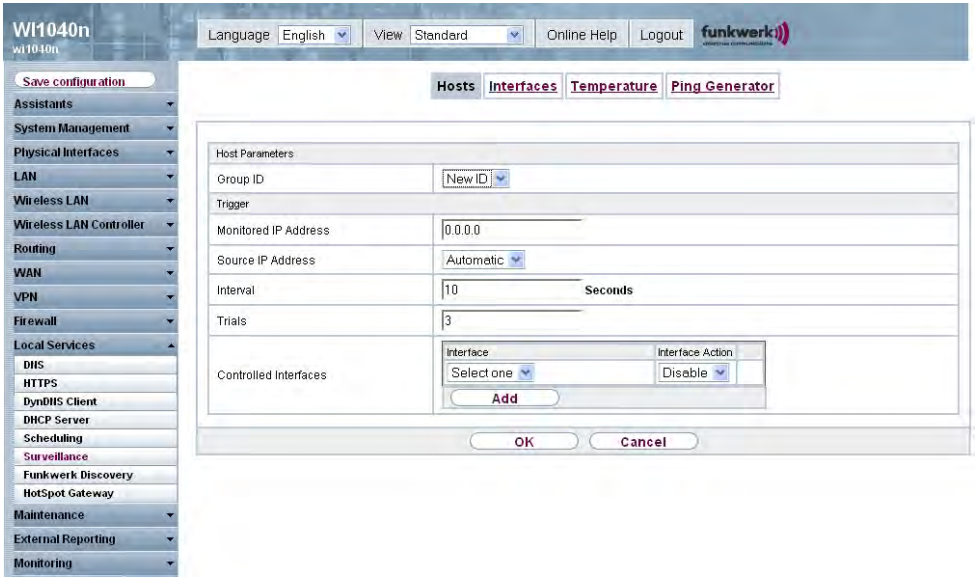


Fig. 146: **Local Services** -> **Surveillance** -> **Hosts** -> **New**

The **Local Services** -> **Surveillance** -> **Hosts** -> **New** menu consists of the following fields:

Fields in the Hosts Host Parameters menu

Field	Description
Group ID	Select an ID for the group of hosts whose availability is to be monitored by your device. The group IDs are automatically created from `0` to `255`. If an entry has not yet been created, a new group is created using the `New ID` option. If entries have been created, you can select one from the list of created groups. Each host to be monitored must be assigned to a group. The action configured in **Interface Action** is only executed if no other group member can be reached.

Fields in the Hosts Trigger menu

Field	Description
Monitored IP Address	Enter the IP address of the host to be monitored.
Source IP Address	Select how the IP address is to be determined that your device

Field	Description
	uses as the source address of the packet sent to the host to be monitored. Possible values: • *Automatic* (default value): The IP address is determined automatically. • *Specific*: Enter the IP address in the adjacent input field.
Interval	Enter the time interval (in seconds) to be used for checking the availability of hosts. Possible values are *1* to *65536*. The default value is *10*. The smallest **Interval** of the group members is used within a group.
Trials	Enter the number of pings that must remain unanswered for the host to be regarded as unavailable. Possible values are *1* to *65536*. The default value is *3*.
Controlled Interfaces	Select the interface(s) for which the action defined in **Interface Action** is to be performed. All physical and virtual interfaces can be selected. For each interface, select whether each interface is to be activated (*Enable*) or deactivated (*Disable*, default value), reset (*Reset*) or if the connection is to be re-established (*Dialup again*).

18.6.2 Interfaces

In the **Local Services** -> **Surveillance** -> **Interfaces** menu, a list of all monitored Interfaces is shown.

18.6.2.1 Edit/New

Choose the icon to edit existing entries. Choose the **New** button to set up monitoring for other interfaces.

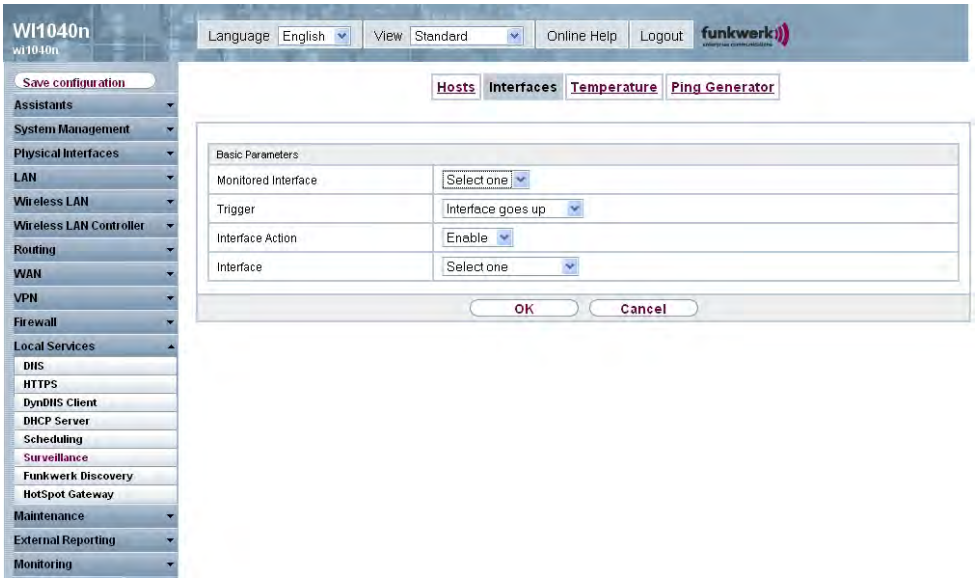


Fig. 147: **Local Services** -> **Surveillance** -> **Interfaces** -> **New**

The **Local Services** -> **Surveillance** ->**Interfaces** -> **New** menu consists of the following fields:

Fields in the Interfaces Basic Parameters menu

Field	Description
Monitored Interface	Select the interface on your device that is to be monitored.
Trigger	Select the state or state transition of **Monitored Interfaces** that is to trigger a particular **Interface Action**. Possible values: • *Interface goes up* (default setting) • *Interface goes down*
Interface Action	Select the action that is to follow the state or state transition defined in **Trigger**.

Field	Description
	The action is applied to the Interface(s) selected in **Interface**. Possible values: • *Enable* (default value): Activation of interface(s) • *Disable*: Deactivation of interface(s)
Interface	Select the interface(s) for which the action defined in **Interface Action** is to be performed. All the physical and virtual interfaces and the options *All PPP Interfaces* and *All IPSec Interfaces* can be selected.

18.6.3 Temperature

The temperature-sensor is only fitted in devices of the **WI series**. It is located on the main board. Its measurement range is from -55 to +125 °C with an accuracy of less than 1 °C.

In the **Local Services** -> **Surveillance** -> **Temperature** menu, a list of all triggers generated is shown. By default, lower and upper limits are set for the temperature; overstepping these sets an alert variable and generates a syslog message. The values are updated every 10 seconds.

18.6.3.1 New

Click on the **New** button to configure new limits.

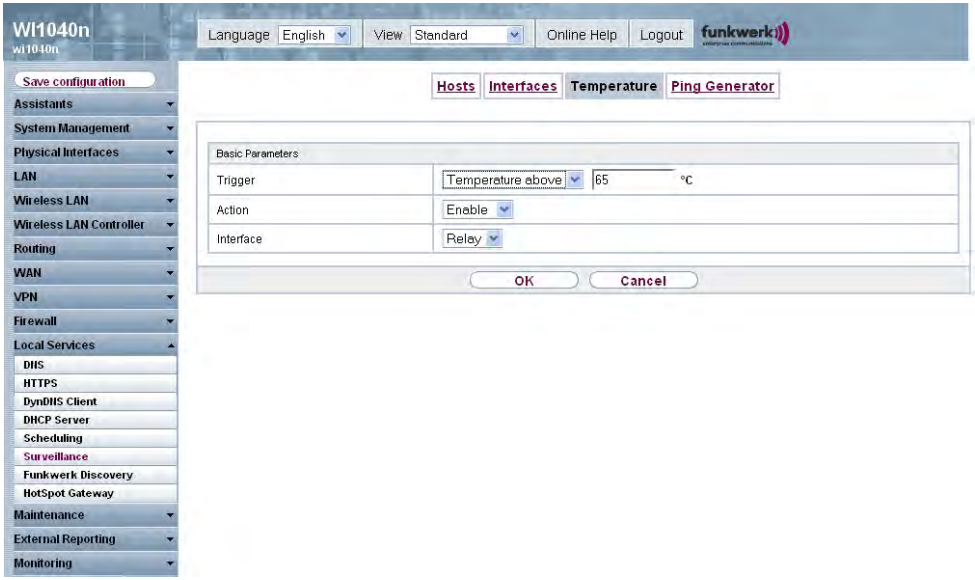


Fig. 148: **Local Services** -> **Surveillance** -> **Temperature** -> **New**

The **Local Services** -> **Surveillance** -> **Temperature** -> **New** menu consists of the following fields:

Fields in the Temperature Basic Parameters menu

Field	Description
Trigger	Enter here the temperature limit value (min/max). Possible values: • *Temperature above* • *Temperature below*
Action	Select the action that is to follow the state or state transition defined in **Trigger**. Possible values: • *Enable* (default value) • *Disable*

Field	Description
Interface	Select the interface via which the action is to be carried out. Possible values: • *Relay* (default value): The overstepping of the limit is coupled with the relay. • *<Interface>*: On overstepping the temperature limit, the selected interface is turned off.

18.6.4 Ping Generator

In the **Local Services** -> **Surveillance** -> **Ping Generator** menu, a list is shown of all pings configured for automatic generation.

18.6.4.1 Edit/New

Choose the icon to edit existing entries. Choose the **New** button to set up further pings.

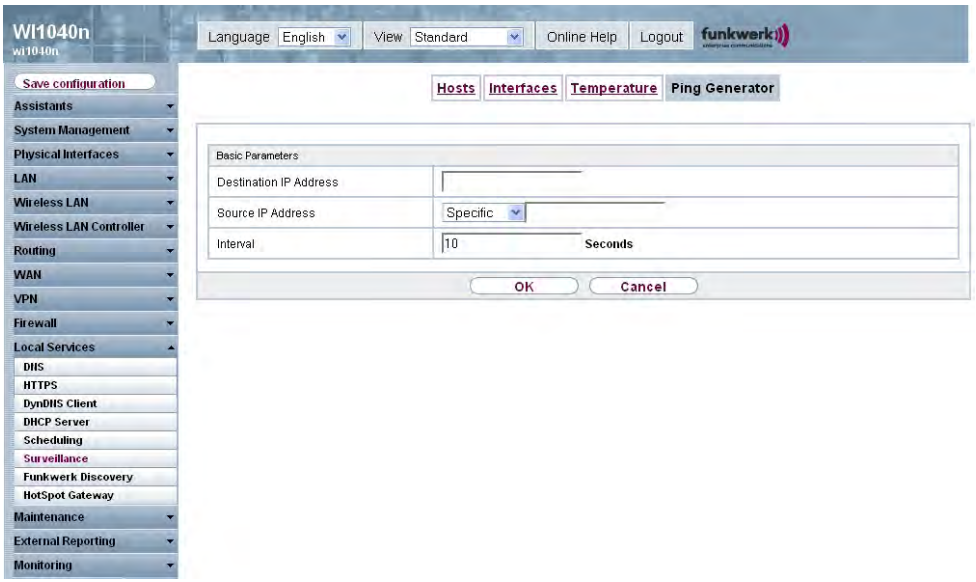


Fig. 149: **Local Services** -> **Surveillance** -> **Ping Generator** -> **New**

The **Local Services** -> **Surveillance** -> **Ping Generator** -> **New** menu consists of the following fields:

Fields in the Ping Generator Basic Parameters menu

Field	Description
Destination IP Address	Enter the IP address to which the ping is automatically sent.
Source IP Address	Enter the source IP address of the outgoing ICMP echo request packets. Possible values: • *Automatic*: The IP address is determined automatically. • *Specific* (default value): Enter the IP address in the adjacent input field e.g. to test a particular extended route.
Interval	Enter the interval is seconds during which the ping is to be sent to the target IPaddress specified in **Target IP Address**. Possible values are *1* to *65536*. The default value is *10*.

18.7 Funkwerk Discovery

18.7.1 Device Discovery

The funkwerk Discovery protocol is used to identify and configure **bintec** access points that are in the same wired network as your device. Once an access point has been discovered, certain basic parameters (node name, IP address, netmask, and device address) can be configured on the access point (provided you know the administrator password).

Note

Any **bintec** access points that exist are determined by means of a multicast. The IP address of the access point is therefore irrelevant.

Please note that the discovered **bintec** access points are not stored in the flash, which means discovery must be repeated after you reboot your device.

In the **Local Services** -> **Funkwerk Discovery** -> **Device Discovery** menu, under **Results** a list is shown of all access points found on the network. In the **Interface** field, select the interface of your device via which access point discovery is to be carried out. You use

the *-All-* option to query all interfaces.

The current discovery status is displayed for each individual interface under Discovery Status. *None* means that discovery is not active. *Discovery* is displayed when discovery is currently being carried out.

This discovery function also enables your device to be discovered and configured by other access points with a discovery function. You configure this in the **Options** sub-menu.

18.7.1.1 Discover

Choose the **Discover** button to start **bintec** access point discovery.

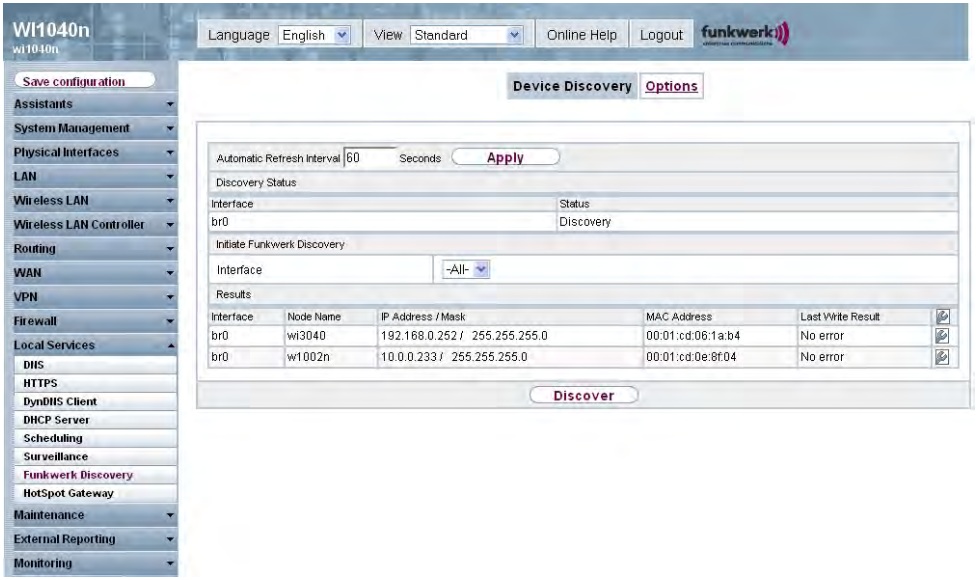


Fig. 150: **Local Services** -> **Funkwerk Discovery** -> **Device Discovery**

If access points were discovered in the network, they are displayed in the list. You use the button to go to the configuration menu for the access point.

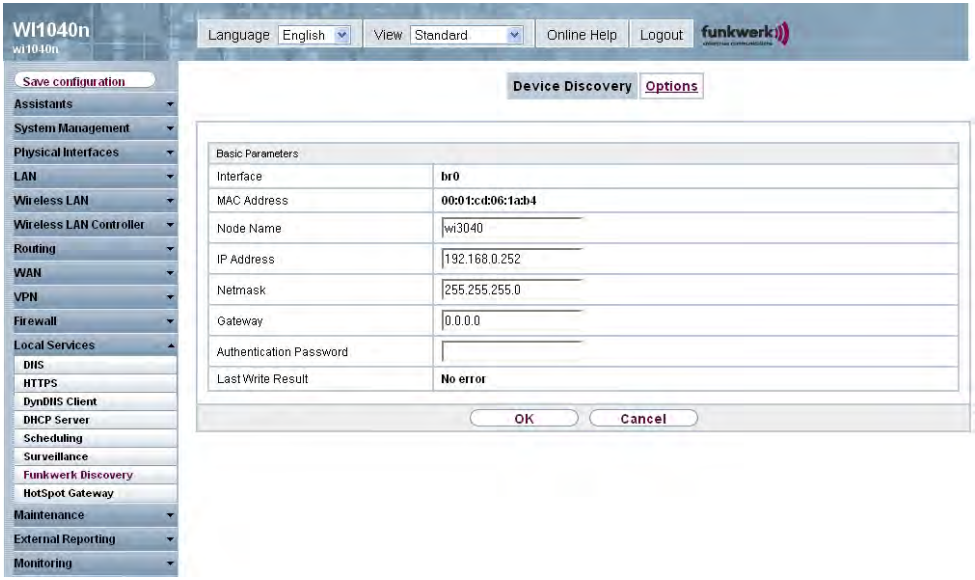


Fig. 151: **Local Services** -> **Funkwerk Discovery** -> **Device Discovery**->

The **Local Services** -> **Funkwerk Discovery** -> **Device Discovery**-> menu consists of the following fields:

Fields in the Device Discovery Basic Parameters

Field	Description
Interface	The value of this field can only be read. Shows the interface of your device on which discovery is carried out.
MAC Address	The value of this field can only be read. Shows the MAC address of the discovered access point.
Node Name	You can change the name of the discovered access point.
IP Address	You can change the IP address of the discovered access point.
Netmask	You can change the related netmask.
Gateway	You can change the gateway address of the discovered access point.

Field	Description
Authentication Password	You must enter the administrator password for the access point, otherwise you cannot carry out the configuration operation.
Last Write Result	The value of this field can only be read. Displays the result of the last configuration operation. Possible values: • *No Error*: The access point reported a successful operation or a configuration change has not yet been made with **OK**. • *No Response*: The access point has not responded. • *Access Denied*: The access point reported an authorisation error. Check the authentication password. • *Invalid IP Parameters*: There is a problem with the intended IP parameters (IP address, netmask, or gateway address). • *Destination Unreachable*: The access point cannot be reached for internal reasons (e.g. the interface to which the access point is connected is down). A configuration request cannot be sent to the access point. • *Other AP Error*: The access point responds to the configuration request with an unexpected or non-specific error. • *Internal Error*: An internal device problem prevented the configuration option from being carried out.

18.7.2 Options

In this menu, you can grant permission for your device to be discovered by other **bintec** devices using the funkwerk Discovery protocol and to be configured by means of this.

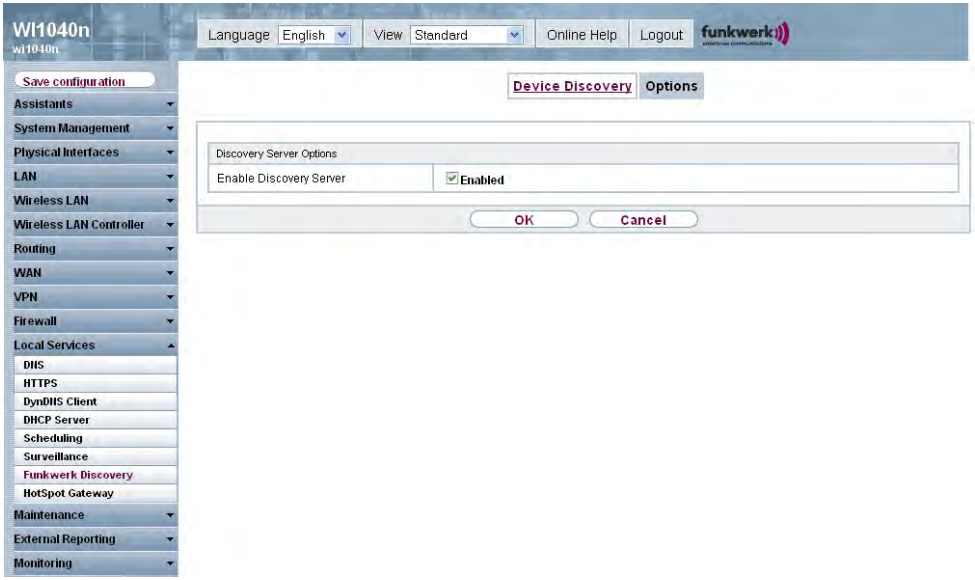


Fig. 152: **Local Services** -> **Funkwerk Discovery** -> **Options**

The **Local Services** -> **Funkwerk Discovery** -> **Options** menu consists of the following fields:

Fields in the Options Discovery Server Options menu

Field	Description
Enable Discovery Server	Select whether your device is to be discovered and configured by other **bintec** devices in the network. The function is activated with *Enabled*. The function is disabled by default.

18.8 Hotspot Gateway

The **bintec HotSpot Solution** allows provision of public Internet accesses (using WLAN or wired Ethernet). The solution is adapted to setup of smaller and larger Hotspot solutions for cafes, hotels, companies, communal residences, campgrounds, etc.

The **bintec HotSpot Solution** consists of a bintec gateway installed onsite (with its own WLAN access point or additional connected WLAN device or wired LAN) and of the Hotspot server, centrally located at a computing centre. The operator account is administered on the server via an administration terminal (e.g., a hotel reception PC); this includes functions such as registration entry, generating tickets, statistical analysis, etc.

Login sequence at the Hotspot server

- When a new user connects with the Hotspot, he/she is automatically assigned an IP address via DHCP.
- As soon as he attempts to access any Internet site with a browser, the user is redirected to the home/login page.
- After the user has entered the registration data (user/password), these are sent to the central RADIUS server (Hotspot server) as RADIUS registration.
- Following successful registration, the gateway opens Internet access.
- For each user, the gateway sends regular additional information to the RADIUS server for recording accounting data.
- When the ticket expires, the user is automatically logged off and again redirected to the home/login page.

Requirements

To operate a Hotspot, the customer requires:

- A bintec device as a Hotspot gateway with an active internet access and configured Hotspot server Entries for login and accounting (see menu **System Management** -> **Remote Authentication** -> **RADIUS** -> **New** with **Group Description** *Standard Group 0*)
- bintec Hotspot hosting (article number 5510000198)
- Access data
- Documentation
- Software licensing

  Please note that you must first activate the licence.

  - Go to *www.funkwerk-ec.com* then **Service/Support** -> **Services** -> **Online Services**.

  - Enter the required data (please note the relevant explanations on the license sheet), and follow the instructions of the online licensing.

  - You then receive the Hotspot server's login data.

Note

Activation may require 2-3 business days.

Access data for gateway configuration

RADIUS Server IP	62.245.165.180
RADIUS Server Password	Set by Funkwerk Enterprise Communications GmbH
Domain	Individually set for customers by customer/dealer
Walled Garden Network	Individually set for customers by customer/dealer
Walled Garden Server URL	Individually set for customers by customer/dealer
Terms & Conditions URL	Individually set for customers by customer/dealer

Access data for configuration of the Hotspot server

Admin URL	https://hotspot.funkwerk-ec.com/
Username	Individually set by FEC
Password	Individually set by FEC

Note

Also refer to the WLAN Hotspot Workshop that is available to download from *www.funkwerk-ec.com* .

18.8.1 Hotspot Gateway

In the **Hotspot Gateway** menu you can configure the bintec gateway installed onsite for the **bintec Hotspot Solution**.

In the **Local Services** -> **Hotspot Gateway** -> **Hotspot Gateway** menu, a list of all configured hotspot networks is shown.

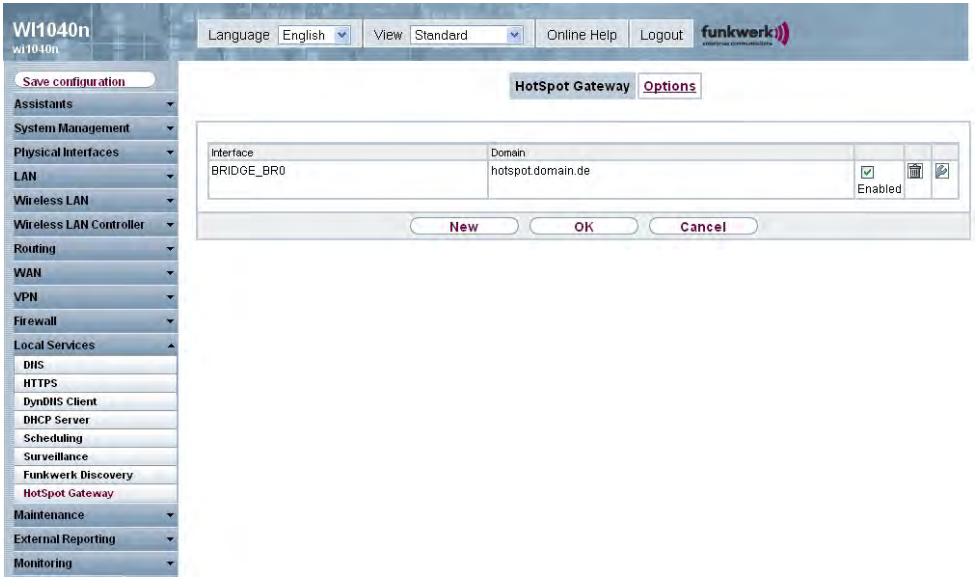


Fig. 153: **Local Services** -> **Hotspot Gateway** -> **Hotspot Gateway** ->

You can use the **Enabled** option to enable or disable the corresponding entry.

18.8.1.1 Edit/New

In the **Local Services** -> **Hotspot Gateway** -> **Hotspot Gateway** -> menu, you configure the Hotspot networks. Choose the **New** button to set up additional Hotspot networks.

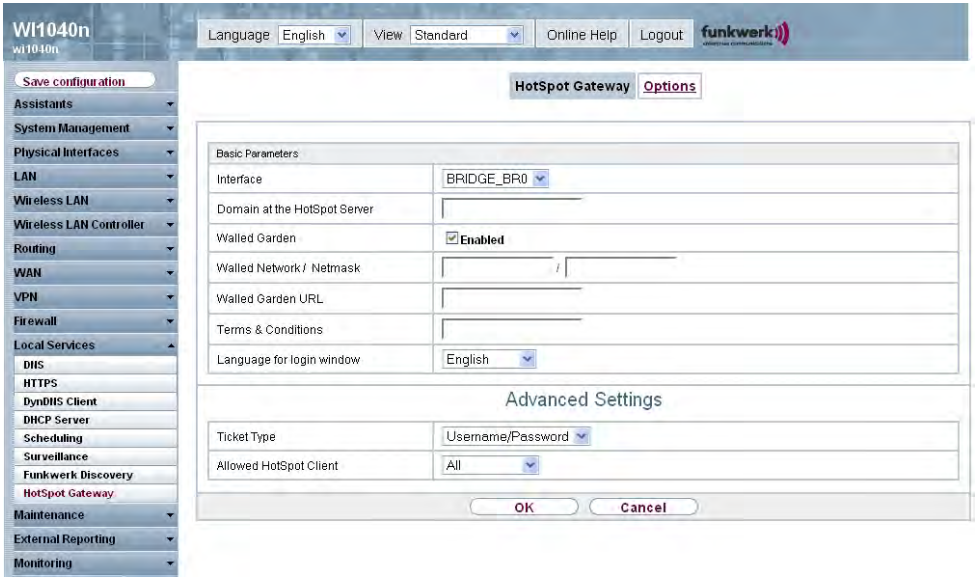


Fig. 154: **Local Services** -> **Hotspot Gateway** -> **Hotspot Gateway** ->

The **Local Services** -> **Hotspot Gateway** -> **Hotspot Gateway** -> menu consists of the following fields:

Fields in the Hotspot Gateway Basic Parameters menu

Field	Description
Interface	Choose the interface to which the Hotspot LAN or WLAN is connected. When operating over LAN, enter the Ethernet interface here (e.g. en1-0). If operating over WLAN, the WLAN interface to which the access point is connected must be selected. **Caution** For security reasons you cannot configure your device over an interface that is configured for the Hotspot. Therefore take care when selecting the interface you want to use for the Hotspot. If you select the interface over which the current configuration session is running, the current connection will be lost. You must then log in again over a reachable interface that is not configured for the Hotspot to configure your device.

Field	Description
Domain at the HotSpot Server	Enter the domain name that you used when setting up the HotSpot server for this customer. The domain name is required so that the Hotspot server can distinguish between the different clients (customers).
Walled Garden	Enable this function if you want to define a limited and free area of websites (intranet). The function is not activated by default.
Walled Network / Netmask	Only if **Walled Garden** is enabled. Enter the network address of the **Walled Network**, the corresponding **Netmask** of the intranet server. For the address range resulting from **Walled Network** / **Netmasks**, clients require no authentication. Example: Enter 192.168.0.0 / 255.255.255.0, if all IP addresses from 192.168.0.0 to 19.168.0.255 are free. Enter 192.168.0.1 / 255.255.255.255, if only the IP address 192.168.0.1 is free.
Walled Garden URL	Only if **Walled Garden** is enabled. Enter the **Walled Garden URL** of the intranet server. Freely accessible websites must be reachable over this address.
Terms & Conditions	Only if **Walled Garden** is enabled. In the **General Terms and Conditions** input field enter the address of the general terms and conditions on the intranet server, or public server, e.g., http://www.webserver.de/agb.htm. The page must lie within the address range of the walled garden network.
Language for login window	Here you can choose the language for the start/login page. The following languages are supported: *English*, *German*, *Italian*, *French*, *Spanish*and *Portuguese*. The language can be changed on the start/login page at any time.

The **Advanced Settings** menu consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Ticket Type	Select the ticket type. Possible values: • *Voucher*: Only the user name must be entered. Define a default password in the input field. • *Username/Password*(default value): User name and password must be entered.
Allowed HotSpot Client	Here you can define which type of users can log in to the Hotspot. Possible values: • *All*: All clients are approved. • *DHCP Client*: Prevents users who have not received an IP address from DHCP from logging in.

18.8.1.2 Options

In the **Local Services** -> **Hotspot Gateway** -> **Options** menu, you configure general settings for the Hotspot.

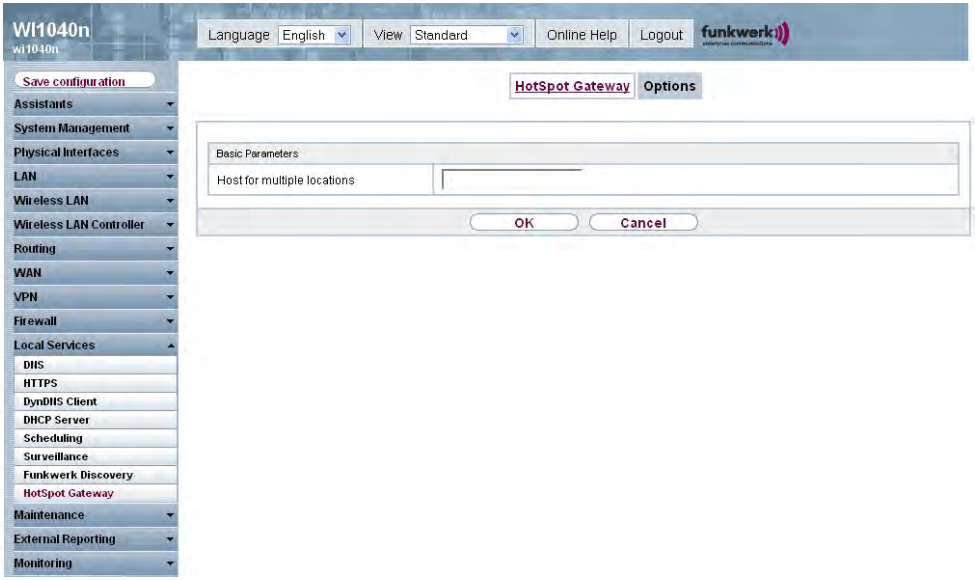


Fig. 155: **Local Services** -> **Hotspot Gateway** -> **Options**

The **Local Services** -> **Hotspot Gateway** -> **Options** menu consists of the following fields:

Fields in the Options Basic Parameters menu

Field	Description
Host for multiple locations	If several locations (branches) are set up on the Hotspot server, enter the value of the NAS identifier (RADIUS server parameter) that has been registered for this location on the Hotspot server.

Chapter 19 Maintenance

This menu provides you with numerous functions for maintaining your device. It firstly provides a menu for testing availability within the network. You can manage your system configuration files. If more recent system software is available, you can use this menu to install it. If you need other languages for the configuration interface, you can import these. You can also trigger a system reboot in this menu.

19.1 Diagnostics

In the **Maintenance** -> **Diagnostics** menu, you can test the accessibility of individual hosts, the resolution of domain names and certain routes.

19.1.1 Ping Test

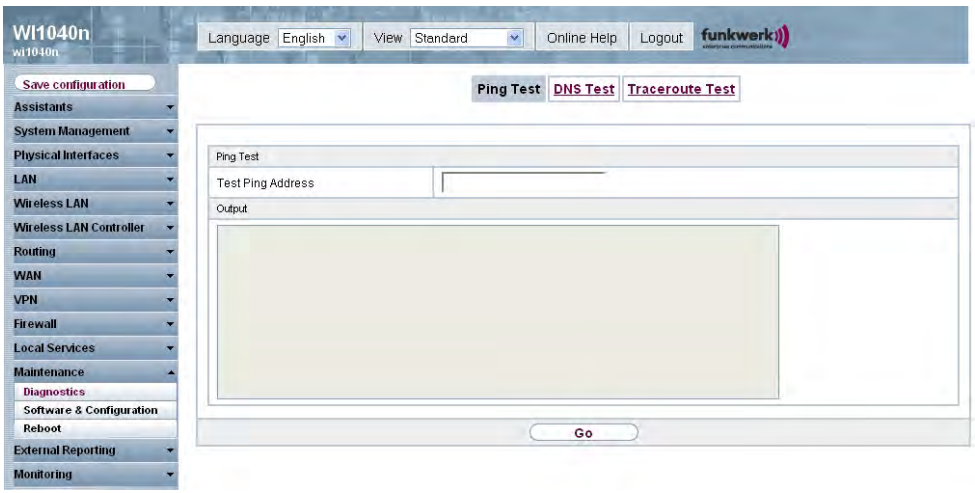


Fig. 156: **Maintenance** -> **Diagnostics** -> **Ping Test**

You can use the ping test to check whether a certain host in the LAN or an internet address can be reached. The **Output** field shows the ping test messages. The ping test is started by entering the IP address to be tested in **Test Ping Address** and clicking on the **Go** button.

19.1.2 DNS Test

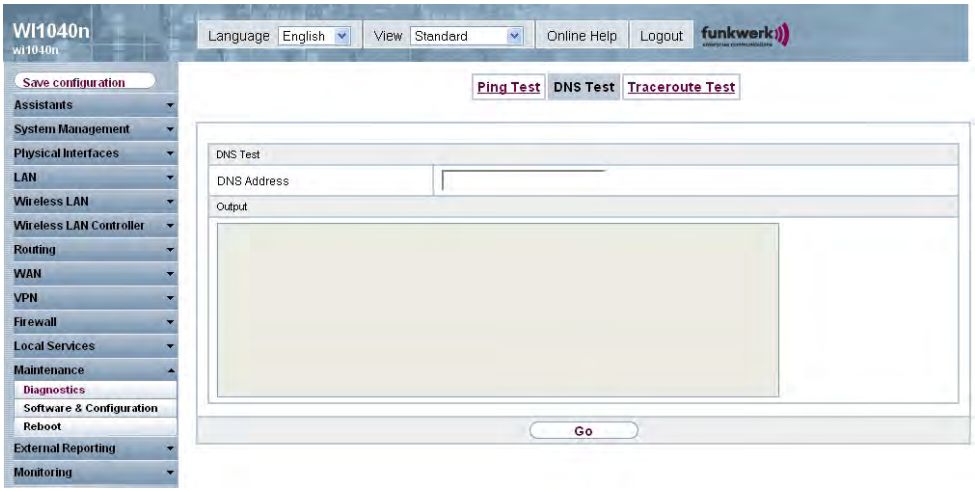


Fig. 157: **Maintenance** -> **Diagnostics** -> **DNS Test**

The DNS test is used to check whether the domain name of a particular host is correctly resolved. The **Output** field shows the DNS test messages. The DNS test is started by entering the domain name to be tested in **DNS Address** and clicking on the **Go** button.

19.1.3 Traceroute Test

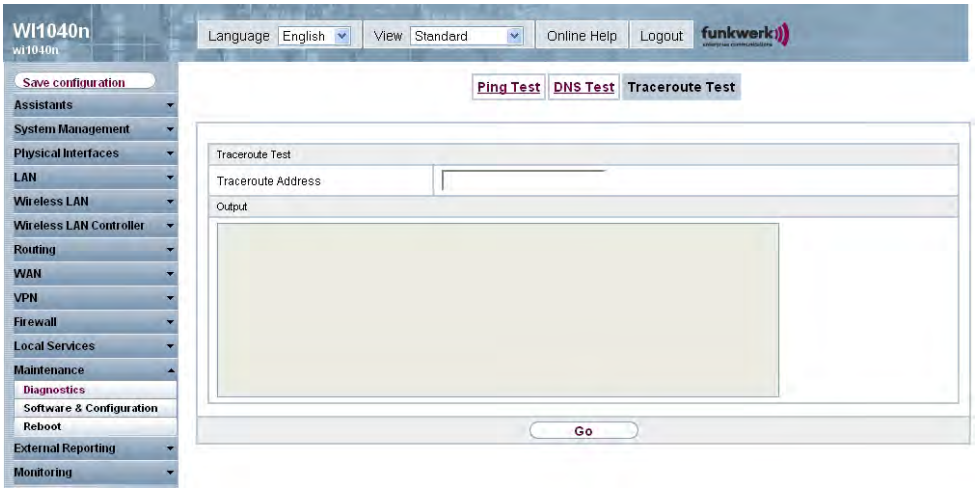


Fig. 158: **Maintenance** -> **Diagnostics** -> **Traceroute Test**

You use the traceroute test to display the route to a particular address (IP address or domain name), if this can be reached. The **Output** field shows the traceroute test messages. The traceroute test is started by entering the address to be tested in **Traceroute Address** and clicking on the **Go** button.

19.2 Software & Configuration

19.2.1 Options

You can use this menu to manage the software version of your device, your configuration files and the language of the **Funkwerk Configuration Interface**.

Your device contains the version of the system software available at the time of production. More recent versions may have since been released. You may therefore need to carry out a software update.

Every new system software includes new features, better performance and any necessary bugfixes from the previous version. You can find the current system software at *www.funkwerk-ec.com*. The current documentation is also available here.

Important

If you want to update your software, make sure you consider the corresponding release notes. These describe the changes implemented in the new system software.

The result of an interrupted update (e.g. power failure during the update) could be that your gateway no longer boots. Do not turn your device off during the update.

An update of BOOTmonitor and/or Logic is recommended in a few cases. In this case, the release notes refer expressly to this fact. Only update BOOTmonitor or Logic if Funkwerk Enterprise Communications GmbH explicitly recommends this.

Flash

Your device saves its configuration in configuration files in the flash EEPROM (Electrically Erasable Programmable Read Only Memory). The data even remains stored in the flash when your device is switched off.

RAM

The current configuration and all changes you set on your device during operation are

stored in the working memory (RAM). The contents of the RAM are lost if the device is switched off. So if you modify your configuration and want to keep these changes for the next time you start your device, you must save the modified configuration in the flash memory before switching off: **Save Configuration** button in the **Funkwerk Configuration Interface** navigation area. This configuration is then saved in the flash in a file with the name *boot*. When you start your device, the *boot* configuration file is used by default.

Operations

The files in the flash memory can be copied, moved, erased and newly created. It is also possible to transfer configuration files between your device and a host via HTTP.

Configuration file format

The file format of the configuration file allows encryption and ensures compatibility when restoring the configuration on the gateway in various system software versions. This is a CSV format, which can be read and modified easily. In addition, you can view the corresponding file clearly using Microsoft Excel for example. The administrator can store encrypted backup files for the configuration. When the configuration is sent by e-mail (e.g for support purposes) confidential configuration data can be protected fully if required. You can save or import files with the actions "Export configuration", "Export configuration with state information" and "Load configuration". If you want to save a configuration file with the action ""Export configuration" or "Export configuration with state information", you can choose whether the configuration file is saved encrypted or without encryption.

Caution

If you have saved a configuration file in an old format via the SNMP shell with the `put` command, there is no guarantee that it can be reloaded to the device. As a result, the old format is no longer recommended.

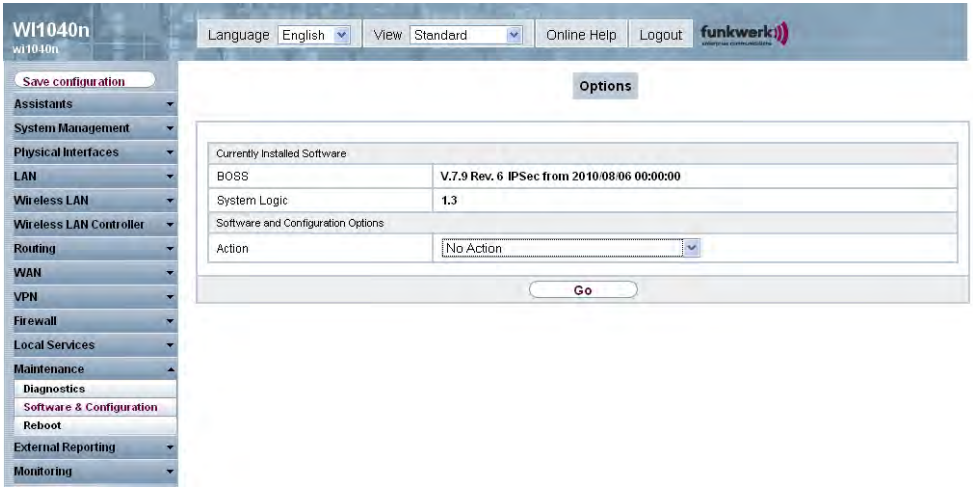


Fig. 159: **Maintenance** -> **Software & Configuration** -> **Options**

The **Maintenance** -> **Software & Configuration** -> **Options** menu consists of the following fields:

Fields in the Options Current Installed Software menu

Field	Description
BOSS	Shows the current software version loaded on your device.
System Logic	Shows the current system logic loaded on your device.
SHDSL Logic	Shows the current version of the SHDSL logic loaded on your device.
ADSL Logic	Shows the current version of the ADSL logic loaded on your device.

Fields in the Options Software and Configuration Options menu

Field	Description
Action	Select the action you wish to execute. After each task, a window is displayed showing the other steps that are required. Possible values: • *No Action* (default value):

Field	Description
	• *Import configuration*: Under **Filename** select a configuration file you want to import. Note: Click **Go** to load the file under the name *boot* in the flash memory for the device. You must restart the device to enable it. Note: The files to be imported must be in CSV format! • *Import language*: You can import other language versions of the **Funkwerk Configuration Interface** into your device. You can download the files to your PC from the download area at *www.funkwerk-ec.com* and from there import them to your device. • *Update system software*: you can start an update of the system software, the ADSL logic and the BOOTmonitor. • *Export configuration*: The configuration file **Current filename in flash memory** is transferred to your local host. If you click on the **Go** button, a dialog box is shown, in which you can select the storage location on your PC and enter the desired file name. • *Export configuration with state information*: The active configuration from the RAM is transferred to your local host. If you click on the **Go** button, a dialog box is shown, in which you can select the storage location on your PC and enter the desired file name. • *Copy*: The configuration file in the **Source File Name** field is saved as **Destination file name**. • *Rename*: The configuration file in the **Select file** field is renamed as **New Filename**. • *Delete configuration*: The configuration file in the **Select file** field is deleted. • *Delete file*: The file in the **Select file** field is deleted.
Configuration Encryption	Only for **Action** = *Import configuration*, *Export configuration*, *Export configuration with state information*. Define whether the data of the selected **Action** are to be encrypted.. The function is activated by choosing *Enabled*. The function is disabled by default. If the function is active, you can enter the **Password** in the text

Field	Description
	field.
Filename	Only for **Action** = *Import configuration*, *Import language*, *Update system software*. Enter the path and name of the file or select the file with **Browse...** via the explorer/finder.
Source Location	Only for **Action** = *Update system software* Select the source for the update. Possible values: • *Local File* (default value): The system software file is stored locally on your PC. • *HTTP server*: The file is stored on a remote server specified in the **URL**. • *Current software from Funkwerk server*: The file is on the official Funkwerk update server.
URL	Only for **Source** = *HTTP server* Enter the URL of the update server from which the system software file is loaded.
Current File Name in Flash	For **Action** = *Export configuration* Choose the configuration file to be exported.
Include certificates and keys	For **Action** = *Export configuration*, *Export configuration with state information*, select whether the selected **Action** is also to apply for certificates and keys. The function is activated by choosing *Enabled*. The function is enabled by default.
Source File Name	Only for **Action** = *Copy*Select the source file to be copied.
Destination File Name	Only for **Action** = *Copy*Enter the name of the copy.
Select file	Only if **Action** = *Rename*, *Delete configuration* or *Delete file*Choose the file or configuration to be renamed or deleted.
New File Name	Only for **Action** = *Rename*Enter the new name of the configura-

Field	Description
	tion file.

19.3 Reboot

19.3.1 System Reboot

In this menu, you can trigger an immediate reboot of your device. Once your system has restarted, you must call the **Funkwerk Configuration Interface** again and log in.

Pay attention to the LEDs on your device. For information on the meaning of the LEDs, see the **Technical Data** chapter of the manual.

Note

Before a reboot, make sure you confirm your configuration changes by clicking the **Save Configuration** button, so that these are not lost when you reboot.

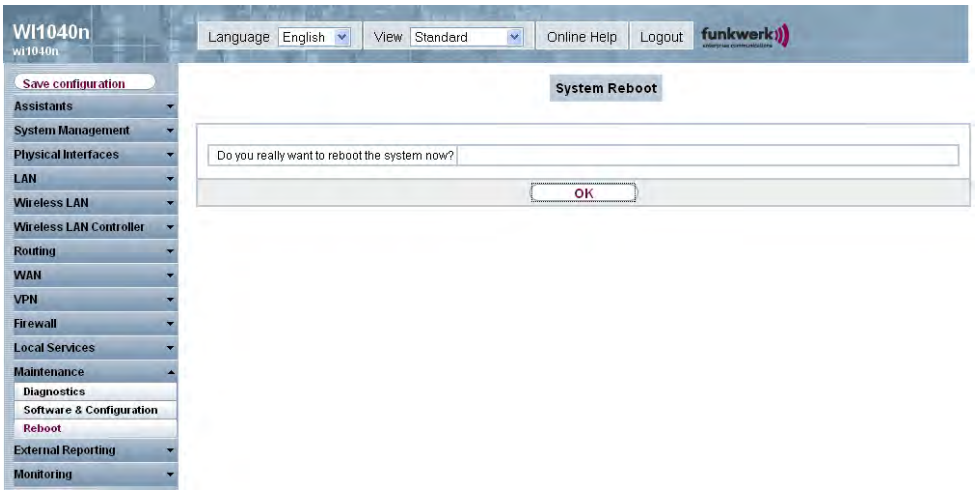


Fig. 160: **Maintenance** -> **Reboot** -> **System Reboot**

If you want to restart your device, click on the **OK** button. The device will reboot.

Chapter 20 External Reporting

In this system menu, you define what system protocol messages are saved on which computers, and whether the system administrator should receive an e-mail for certain events. Information on IP data traffic can also be saved--depending on the individual interfaces. In addition, SNMP traps can be sent to specific hosts in case of error. Moreover, you can prepare your device for monitoring with the activity monitor.

20.1 Syslog

Events in various subsystems of your device (e.g. PPP) are logged in the form of syslog messages (system logging messages). The number of messages visible depends on the level set (eight levels from *Emergency* and *Information* to *Debug*).

In addition to the data logged internally on your device, all information can and should also be passed to one or more external PCs for storage and processing, e.g. to the system administrator's PC. The syslog messages saved internally on your device are lost when you reboot.

Warning

Make sure you only pass syslog messages to a safe computer. Check the data regularly and ensure that there is always enough spare capacity available on the hard disk of your PC.

Syslog Daemon

All Unix operating systems support the recording of syslog messages. For Windows PCs, the Syslog Demon included in the **DIME Tools** can record the data and distribute to various files depending on the contents (can be called in the download area at *www.funkwerk-ec.com*).

20.1.1 Syslog Servers

Configure your device as a syslog server so that defined system messages can be sent to suitable hosts in the LAN.

In this menu, you define which messages are sent to which hosts and with which conditions.

In the **External Reporting** -> **Syslog** -> **Syslog Servers** menu, a list of all configured system log servers is shown.

20.1.1.1 New

Choose the **New** button to set up new syslog servers.

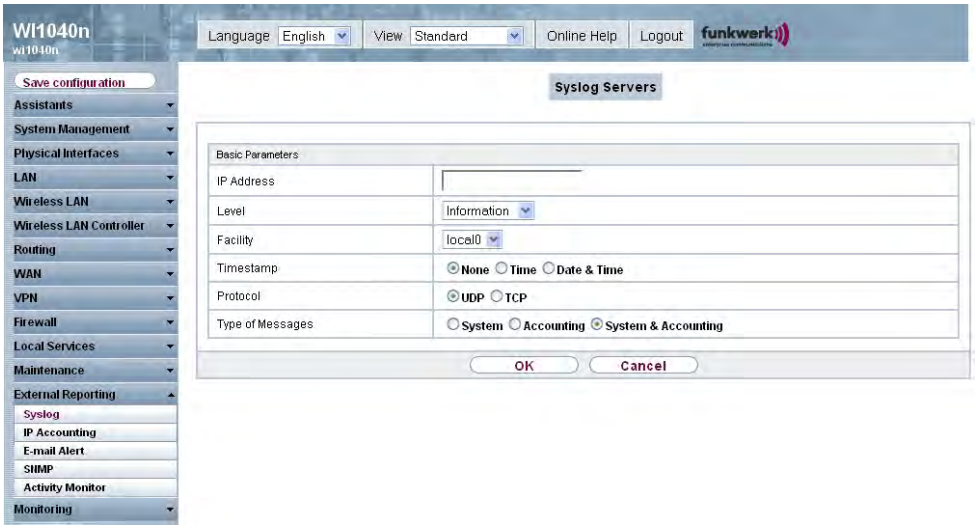


Fig. 161: **External Reporting** -> **Syslog** -> **Syslog Servers** -> **New**

The **External Reporting** -> **Syslog** -> **Syslog Servers** -> **New** menu consists of the following fields:

Fields in the Syslog Servers Basic Parameters menu

Field	Description
IP Address	Enter the IP address of the host to which syslog messages are passed.
Level	Select the priority of the syslog messages that are to be sent to the host. Possible values: • *Emergency* (highest priority) • *Alert* • *Critical* • *Error*

Field	Description
	• *Warning* • *Notice* • *Information* (default value) • *Debug* (lowest priority) Syslog messages are only sent to the host if they have a higher or identical priority to that indicated, i.e. all messages generated are recorded at syslog level *Debug*.
Facility	Enter the syslog facility on the host. This is only required if the **Log Host** is a Unix computer. Possible values: *local0 - 7* . The default value is *local0*.
Timestamp	Select the format of the time stamp in the syslog. Possible values: • *None* (default value): No system time indicated. • *Time* : System time without date. • *Date & Time* : System time with date.
Protocol	Select the protocol for the transfer of syslog messages. Note that the syslog server must support the protocol. Possible values: • *UDP* (default value) • *TCP*
Type of Messages	Select the message type. Possible values: • *System & Accounting* (default value) • *System* • *Accounting*

20.2 IP Accounting

In modern networks, information about the type and number of data packets sent and received over the network connections is often collected for commercial reasons. This information is extremely important for Internet Service Providers that bill their customers by data volume.

However, there are also non-commercial reasons for detailed network accounting. If, for example, you manage a server that provides different kinds of network services, it is useful for you to know how much data is generated by the individual services.

Your device contains the IP Accounting function, which enables you to collect a lot of useful information about the IP network traffic (each individual IP session).

20.2.1 Interfaces

In this menu, you can configure the IP Accounting function individually for each interface.

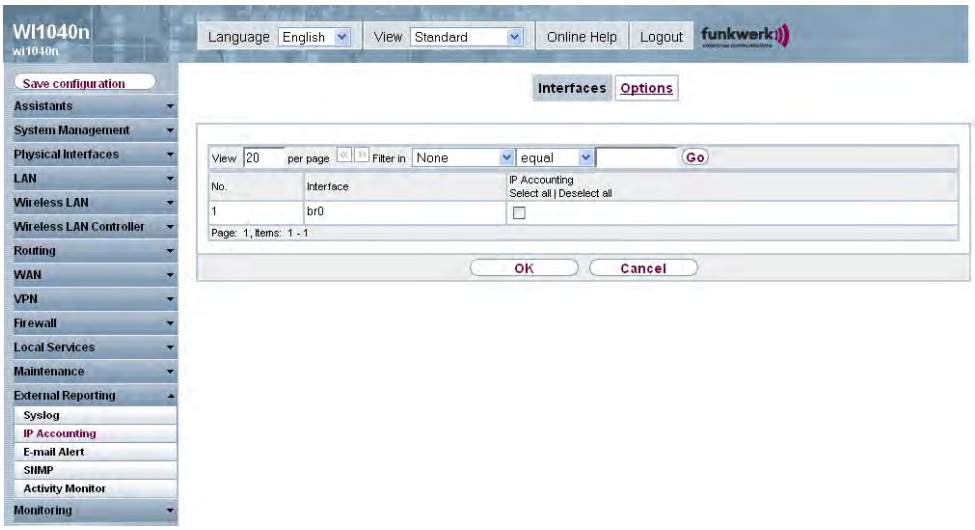


Fig. 162: **External Reporting** -> **IP Accounting** -> **Interfaces**

In the **External Reporting** -> **IP Accounting** -> **Interfaces** menu, a list of all interfaces configured on your device is shown. For each entry, you can activate IP Accounting by setting the checkmark. In the **IP Accounting** column, you do not need to click each entry individually. Using the options **Select All** and **Disable All**, you can enable or disable the IP accounting function for all interfaces simultaneously.

20.2.2 Options

In this menu, you configure general settings for IP Accounting.

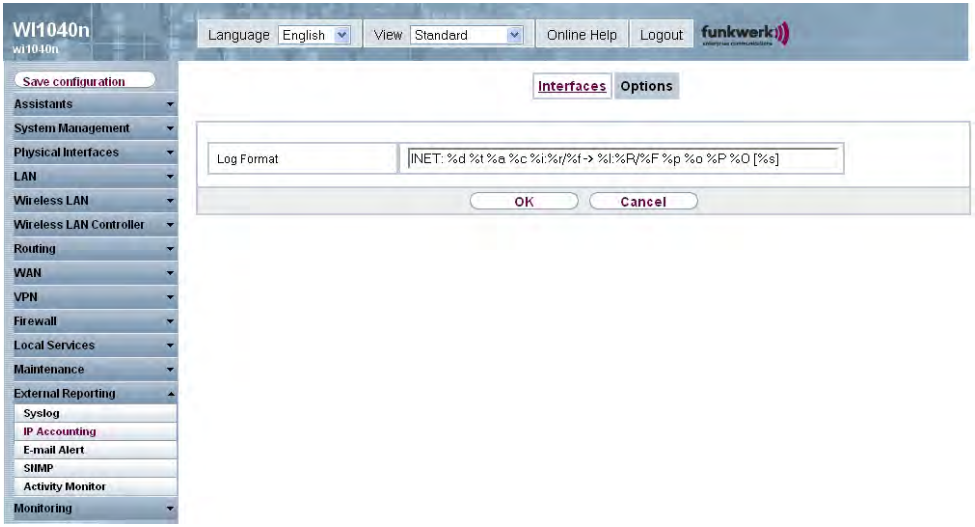


Fig. 163: **External Reporting** -> **IP Accounting** -> **Options**

In the **External Reporting** -> **IP Accounting** -> **Options** menu you can set the **Log Format** of the IP accounting messages. The messages can contain character strings in any order, sequences separated by a slash, e.g. `\t` or `\n` or defined tags.

Possible format tags:

Format tags for IP accounting messages

Field	Description
%d	Date of the session start in the format DD.MM.YY
%t	Time of the session start in the format HH:MM:SS
%a	Duration of the session in seconds
%c	Protocol
%i	Source IP Address
%r	Source Port
%f	Source interface index
%I	Destination IP Address
%R	Destination Port
%F	Destination interface index

Field	Description
%p	Packets sent
%o	Octets sent
%P	Packets received
%O	Octets received
%s	Serial Number for accounting message
%%	%

By default, the following format instructions are entered in the **Log Format** field. *INET: %d%t%a%c%i:%r/%f -> %I:%R/%F%p%o%P%O[%s]*

20.3 E-mail Alert

Depending on the configuration, E-mails are sent to the administrator as soon as relevant syslog messages occur.

20.3.1 E-mail Alert Server

The **E-mail Alert Server** menu consists of the following fields:

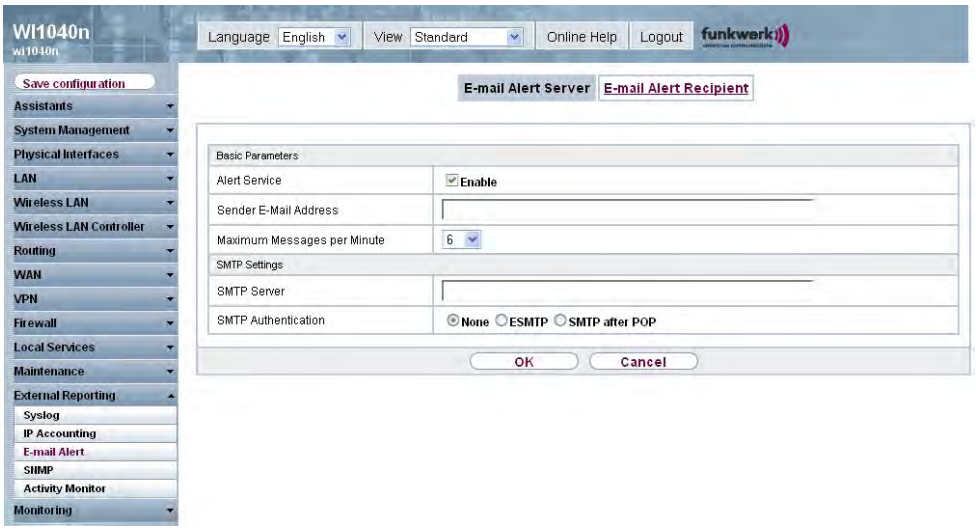


Fig. 164: **External Reporting** -> **E-mail Alert** -> **E-mail Alert Server**

The **External Reporting** -> **E-mail Alert** -> **E-mail Alert Server** menu consists of the following fields:

Fields in the E-mail Alert Server Basic Parameters menu

Field	Description
Alert Service	Enable or disable the function.
Sender E-Mail Address	Enter the mail address to be entered in the sender field of the E-mail.
Maximum Messages per Minute	Limit the number of outgoing mails per minute. Possible values are *1* to *15*, the default value is *6*.

Fields in the E-mail Alert Server SMTP Settings menu

Field	Description
SMTP Server	Enter the address (IP address or valid DNS name) of the mail server to be used for sending the mails. The entry is limited to 40 characters.
SMTP Authentication	Authentication expected by the SMTP server. Possible values: • *None* (default value): The server accepts and send emails without further authentication. • *ESMTP*: The server only accepts emails if the router is logged in with the correct user name and password. • *SMTP after POP*: The server requires that emails are called via POP3 by the sending IP with the correct POP3 user name and password before sending an email.
User Name	Only if **SMTP Authentication** = *ESMTP* or *SMTP after POP*. Enter the user name for the POP3 or SMTP server.
Password	Only if **SMTP Authentication** = *ESMTP* or *SMTP after POP*. Enter the password of this user.
POP3 Server	Only if **SMTP Authentication** = *SMTP after POP*. Enter the address of the server from which the e-mails are to be retrieved.
POP3 Timeout	Only if **SMTP Authentication** = *SMTP after POP*. Enter how long the router must wait after the POP3 call before it is forced to send the alert mail.

Field	Description
	The default value is `600` seconds.

20.3.2 E-mail Alert Recipient

In the **E-mail Alert Recipient** menu, a list of syslog messages is displayed.

20.3.2.1 New

Choose the **New** button to create new e-mail alert receivers.

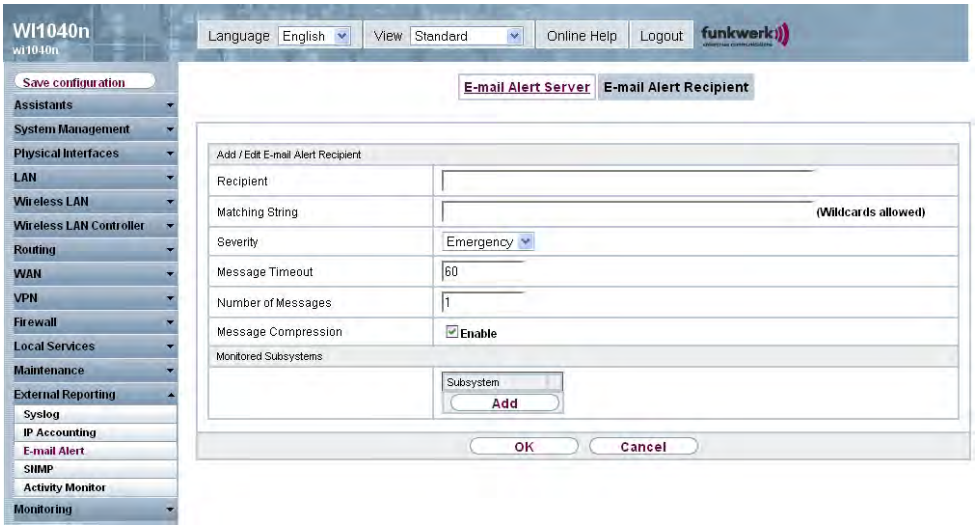


Fig. 165: **External Reporting** -> **E-mail Alert**-> **E-mail Alert Recipient**

The **External Reporting** -> **E-mail Alert** -> **E-mail Alert Recipient** menu consists of the following fields:

Fields in the E-mail Alert Receiver Add / Edit E-mail Alert Recipient menu

Field	Description
Recipient	Enter the E-mail address of the recipient. The entry is limited to 40 characters.
Matching String	You must enter a "Matching String". This must occur in a syslog message as a necessary condition for triggering an alert. The entry is limited to 55 characters. Bear in mind that without the use of wildcards (e.g. "*"), only those strings that correspond exactly to the entry fulfil the condition. The "Matching String"

Field	Description
	entered therefore usually contains wildcards. To be informed of all syslog messages of the selected level, just enter "*".
Severity	Select the severity at which the string configured in the **Matching String** field must occur to trigger an E-mail alert. Possible values: *Emergency* (default value), *Alert*, *Critical*, *Error*, *Warning*, *Notice*, *Information*, *Debug*
Message Timeout	Enter how long the router must wait after a relevant event before it is forced to send the alert mail. Possible values are *0* to *86400*. The value 0 disables the timeout.
Number of Messages	Enter the number of syslog messages that must be reached before an E-mail can be sent for this case. If timeout is configured, the mail is sent when this expires, even if the number of messages has not been reached. Possible values are *0* to *99*; the default value is *1*.
Message Compression	Select whether the text in the alert E-mail is to be shortened. The e-mail then contains the syslog message only once plus the number of relevant events. Enable or disable the field. The function is enabled by default.

Fields in the E-mail Alert Recipient Monitored Subsystems menu

Field	Description
Subsystem	Select the subsystems to be monitored. Add a new system with **Add**.

20.4 SNMP

SNMP (Simple Network Management Protocol) is a protocol from the IP protocol family for transporting management information about network components.

Every SNMP management system contains an MIB. SNMP can be used to configure, control and administrate various network components from one system. Such an SNMP tool is included on your device: the Configuration Manager. As SNMP is a standard protocol, you can use any other SNMP managers, e.g. HPOpenView.

For more information on the SNMP versions, see the relevant RFCs and drafts:

- SNMP V. 1: RFC 1157
- SNMP V. 2c: RFC 1901 - 1908
- SNMP V. 3: RFC 3410 - 3418

20.4.1 SNMP Trap Options

In the event of errors, a message - known as a trap packet - is sent unrequested to monitor the system.

In the **External Reporting** -> **SNMP** -> **SNMP Trap Options** menu, you can configure the sending of traps.

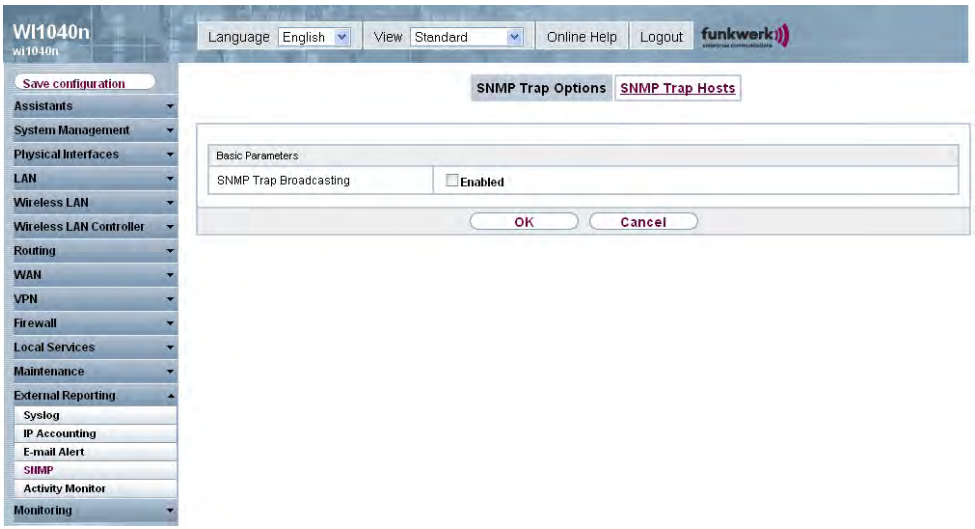


Fig. 166: **External Reporting** -> **SNMP** -> **SNMP Trap Options**

The **External Reporting** -> **SNMP** -> **SNMP Trap Options** menu consists of the following fields:

Fields in the SNMP Trap Options Basic Parameters menu

Field	Description
SNMP Trap Broadcasting	Select whether the transfer of SNMP traps is to be activated. Your device then sends SNMP traps to the LAN's broadcast address. The function is activated by choosing *Enabled*. The function is disabled by default.
SNMP Trap UDP Port	Only if **SNMP Trap Broadcasting** is enabled. Enter the number of the UDP port to which your device is to send SNMP traps. Any whole number is possible. The default value is *162*.
SNMP Trap Community	Only if **SNMP Trap Broadcasting** is enabled. Enter a new SNMP code. This must be sent by the SNMP Manager with every SNMP request so that this is accepted by your device. A character string of between *0* and *255* characters is possible here. The default value is *SNMP Trap*.

20.4.2 SNMP Trap Hosts

In this menu, you specify the IP addresses to which your device is to send the SNMP traps.

In the **External Reporting** -> **SNMP** -> **SNMP Trap Hosts** menu, a list of all configured SNMP trap hosts is shown.

20.4.2.1 New

Choose the **New** button to set up new SNMP trap hosts.

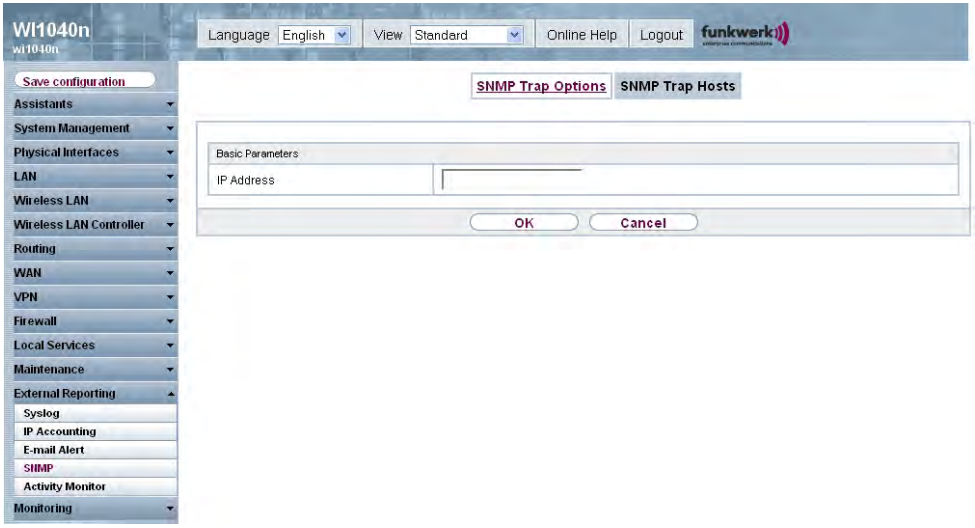


Fig. 167: **External Reporting** -> **SNMP** -> **SNMP Trap Hosts** -> **New**

The **External Reporting** -> **SNMP** -> **SNMP Trap Hosts** -> **New** menu consists of the following fields:

Fields in the SNMP Trap Hosts Basic Parameters menu

Field	Description
IP Address	Enter the IP address of the SNMP trap host.

20.5 Activity Monitor

This menu contains the settings needed to monitor your device with the Windows tool **Activity Monitor** (part of **BRICKware** for Windows).

Purpose

The **Activity Monitor** enables Windows users to monitor the activities of your device. Important information about the status of physical interfaces (e.g. ISDN line) and virtual interfaces is easily obtained with one tool. A permanent overview of the utilisation of your device is possible.

Method of operation

A Status Daemon collects information about your device and transfers it as UDP packets to the broadcast address of the first LAN interface (default setting) or to an explicitly entered

IP address. One packet is sent per time interval, which can be adjusted individually to values from 1 - 60 seconds. Up to 100 physical and virtual interfaces can be monitored, provided the packet size of 4096 bytes is not exceeded. The **Activity Monitor** on your PC receives the packets and can display the information contained in them in various ways according to the configuration.

Activate the **Activity Monitor** as follows:

- configure the relevant device(s) to be monitored.
- Start and configure the Windows application on your PC (you can download **BRICKware** for Windows to your PC from the download area at *www.funkwerk-ec.com* and from there import it to your device).

20.5.1 Options

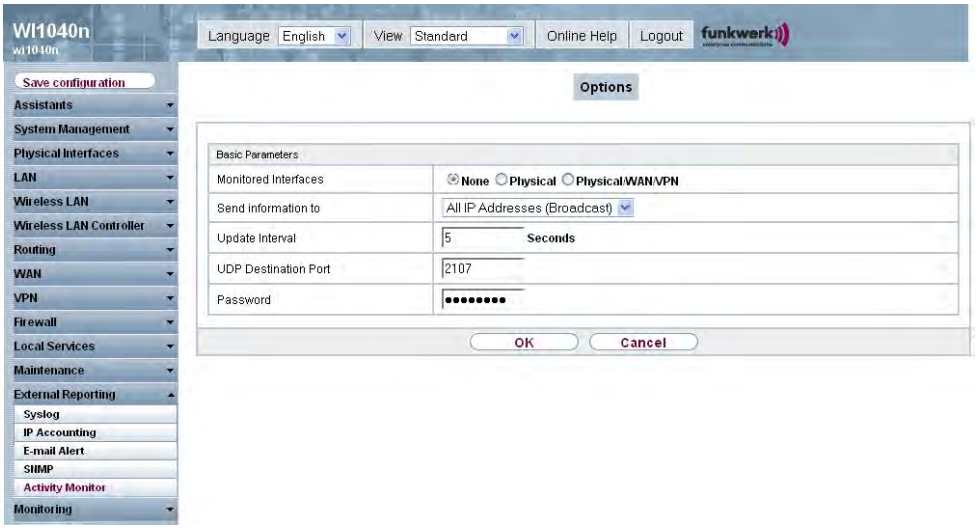


Fig. 168: **External Reporting** -> **Activity Monitor** -> **Options**

The **External Reporting** -> **Activity Monitor** -> **Options** menu consists of the following fields:

Fields in the Options Basic Parameters menu

Field	Description
Monitored Interfaces	Select the type of information to be sent in the UDP packets to the Windows application. Possible values:

Field	Description
	• *None* (default value): Deactivates the sending of information to the **Activity Monitor**. • *Physical*: Only information about the physical interfaces is sent. • *Physical/WAN/VPN*: Information about physical and virtual interfaces is sent
Send information to	Select where your device sends the UDP packets. Possible values: • *All IP Addresses (broadcast)* (default value): The default value *255.255.255.255* means that the broadcast address of the first LAN interface is used. • *Single Host*: The UDP packets are sent to the IP address entered in the adjacent input field.
Update Interval	Enter the update interval (in seconds). Possible values are *0* to *60*. The default value is *5*.
UDP Destination Port	Enter the port number for the Windows application **Activity Monitor**. The default value is *2107* (registered by IANA - Internet Assigned Numbers Authority).
Password	Enter the password for the **Activity Monitor**.

Chapter 21 Monitoring

This menu contains information that enable you to locate problems in your network and monitor activities, e.g. at your device's WAN interface.

21.1 Internal Log

21.1.1 System Messages

In the **Monitoring** -> **Internal Log** -> **System Messages** menu, a list of all internally stored system messages is shown. Above the table you will find the configured **Maximum Number of Syslog Entries** and the configured **Maximum Message Level of Syslog Entries**. These values can be changed in the **System Management** -> **Global Settings** -> **System** menu.

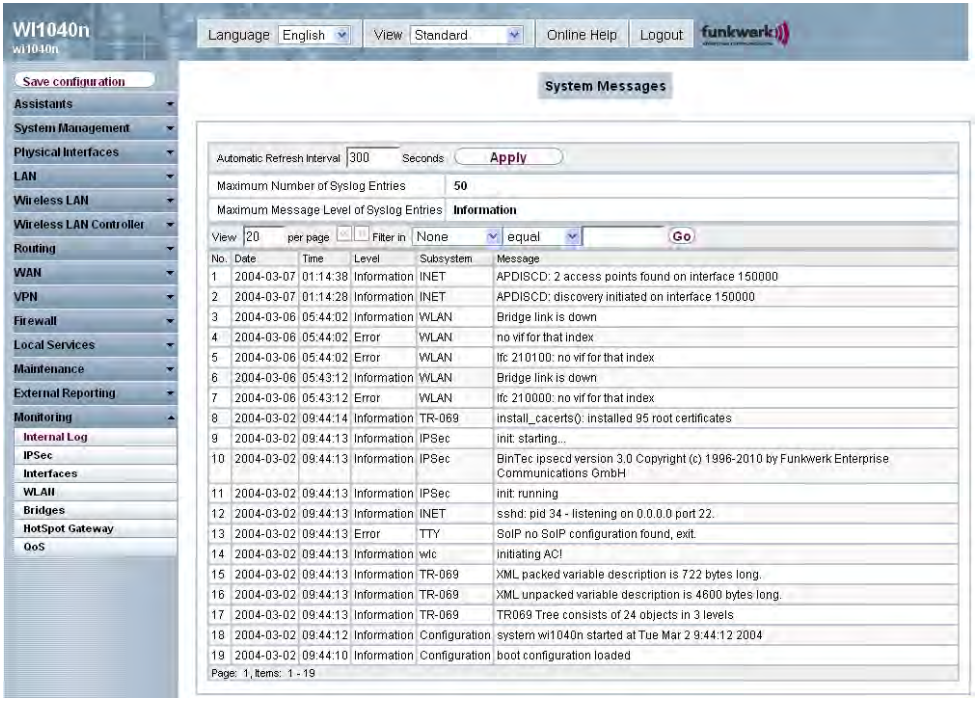

WI1040n
Language English
View Standard
Online Help
Logout
Save configuration
Assistants
System Management
Physical Interfaces
LAN
Wireless LAN
Wireless LAN Controller
Routing
WAN
VPN
Firewall
Local Services
Maintenance
External Reporting
Monitoring
Internal Log
IPSec
Interfaces
WLAN
Bridges
HotSpot Gateway
QoS
System Messages
Automatic Refresh Interval 300 Seconds Apply
Maximum Number of Syslog Entries 50
Maximum Message Level of Syslog Entries Information
View 20 per page Filter in None equal Go
No. Date Time Level Subsystem Message
1 2004-03-07 01:14:38 Information INET APDISCD: 2 access points found on interface 150000
2 2004-03-07 01:14:28 Information INET APDISCD: discovery initiated on interface 150000
3 2004-03-06 05:44:02 Information WLAN Bridge link is down
4 2004-03-06 05:44:02 Error WLAN no vif for that index
5 2004-03-06 05:44:02 Error WLAN Ifc 210100: no vif for that index
6 2004-03-06 05:43:12 Information WLAN Bridge link is down
7 2004-03-06 05:43:12 Error WLAN Ifc 210000: no vif for that index
8 2004-03-02 09:44:14 Information TR-069 install_cacerts(): installed 95 root certificates
9 2004-03-02 09:44:13 Information IPSec init: starting...
10 2004-03-02 09:44:13 Information IPSec BinTec ipsecd version 3.0 Copyright (c) 1996-2010 by Funkwerk Enterprise Communications GmbH
11 2004-03-02 09:44:13 Information IPSec init: running
12 2004-03-02 09:44:13 Information INET sshd: pid 34 - listening on 0.0.0.0 port 22.
13 2004-03-02 09:44:13 Error TTY SoIP no SoIP configuration found, exit.
14 2004-03-02 09:44:13 Information wlc initiating AC!
15 2004-03-02 09:44:13 Information TR-069 XML packed variable description is 722 bytes long.
16 2004-03-02 09:44:13 Information TR-069 XML unpacked variable description is 4600 bytes long.
17 2004-03-02 09:44:13 Information TR-069 TR069 Tree consists of 24 objects in 3 levels
18 2004-03-02 09:44:12 Information Configuration system wi1040n started at Tue Mar 2 9:44:12 2004
19 2004-03-02 09:44:10 Information Configuration boot configuration loaded
Page: 1, Items: 1 - 19

Fig. 169: **Monitoring** -> **Internal Log** -> **System Messages**

Values in the list System Messages

Field	Description
No.	Displays the serial number of the system message.
Date	Displays the date of the record.
Time	Displays the time of the record.
Level	Displays the hierarchy level of the message.
Subsystem	Displays which subsystem of the device generated the message.
Message	Displays the message text.

21.2 IPSec

21.2.1 IPSec Tunnels

In the **Monitoring** -> **IPSec** -> **IPSec Tunnel** menu, a list of all configured IPSec peers is shown.

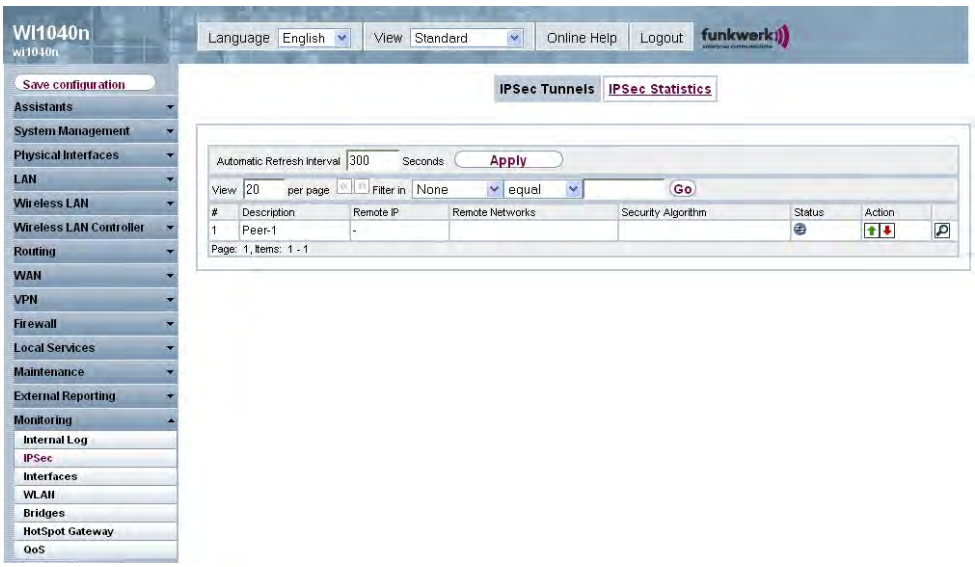


Fig. 170: **Monitoring** -> **IPSec** -> **IPSec Tunnel**

Values in the list IPSec Tunnels

Field	Description
#	Displays the serial number of the IPSec tunnel.
Description	Displays the name of the IPSec tunnel.

Field	Description
Remote IP Address	Displays the IP address of the remote IPSec Peers.
Remote Networks	Displays the currently negotiated subnets of the remote terminal.
Security Algorithm	Displays the encryption algorithm of the IPSec tunnel.
Status	Displays the operating status of the IPSec tunnel.
Action	Enables you to change the status of the IPSec tunnel as displayed.
Details	Opens a detailed statistics window.

You change the status of the IPSec tunnel by pressing the button or button in the **Action** column.

By pressing the button, you display detailed statistics on the IPSec connection.

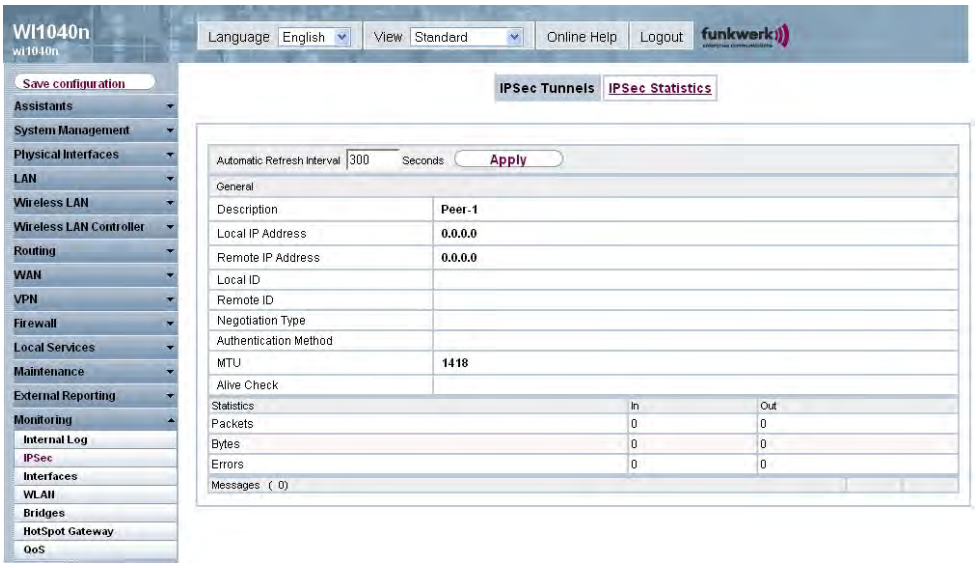


Fig. 171: **Monitoring** -> **IPSec** -> **IPSec Tunnel**->

Values in the list IPSec Tunnels

Field	Description
Description	Shows the description of the peer.
Local IP Address	Shows the WAN IP address of your device.
Destination IP Address	Shows the WAN IP address of the connection partner.
Local ID	Shows the ID of your device for this IPSec tunnel.

Field	Description
Remote ID	Shows the ID of the peer.
Negotiation Type	Shows the exchange type.
Authentication Method	Shows the authentication method.
MTU	Shows the current MTU (Maximum Transfer Unit).
Alive Check	Shows the method for checking that the peer is reachable.
NAT Detection	Displays the NAT detection method.
Local Port	Shows the local port.
Remote Port	Shows the remote port.
Packets	Shows the total number of incoming and outgoing packets.
Bytes	Shows the total number of incoming and outgoing bytes.
Errors	Shows the total number of errors.
IKE (Phase 1) SAs (x) Role / Algorithm / Lifetime remaining / State	The parameters of the IKE (Phase 1) SAs are displayed here.
IPSec (Phase 2) SAs (x) Role / Algorithm / Local / Remote / Lifetime remaining / State	Shows the parameters of the IPSec (Phase 2) SAs.
Messages	The system messages for this IPSec tunnel are displayed here.

21.2.2 IPSec Statistics

In the **Monitoring** -> **IPSec** -> **IPSec Statistics** menu, statistical values for all IPSec connections are shown.

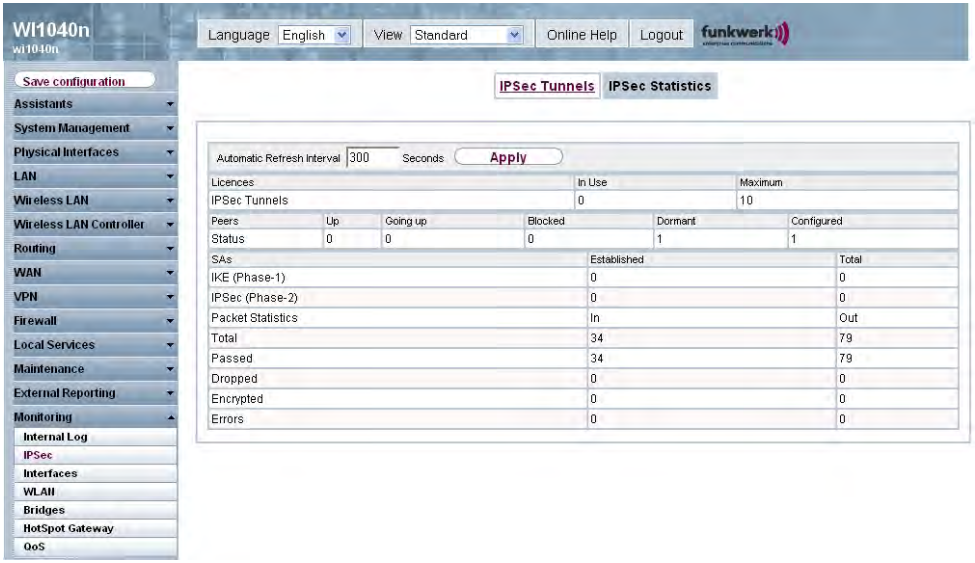


Fig. 172: **Monitoring** -> **IPSec** -> **IPSec Statistics**

The **Monitoring** -> **IPSec** -> **IPSec Statistics** menu consists of the following fields:

Field in the IPSec Statistics Licenses menu

Field	Description
IPSec Tunnels	Shows the IPSec licenses currently in use (**In use**) and the maximum number of licenses usable (**Maximum**).

Field in the IPSec Statistics Peers menu

Field	Description
Status	Displays the number of IPSec tunnels by their current status. • **Active**: Currently active IPSec tunnels. • **Enable**: IPSec tunnels currently in the tunnel setup phase. • **Blocked**: IPSec tunnels that are blocked. • **Dormant**: Currently inactive IPSec tunnels. • **Configured**: Configured IPSec tunnels.

Field in the IPSec Statistics SAs menu

Field	Description
IKE (Phase1)	Shows the number of active phase-1 SAs (**Established**) from the total number of phase-1 SAs (**Total**).
IPSec (Phase2)	Shows the number of active phase-2 SAs (**Established**) from

Field	Description
	the total number of phase-2 SAs (**Total**).

Field in the IPSec Statistics Packet Statistics menu

Field	Description
Total	Shows the number of all processed incoming (**Incoming**) or outgoing (**Outgoing**) packets.
Passed	Shows the number of incoming (**Incoming**) or outgoing (**Outgoing**) packets forwarded in plain text.
Dropped	Shows the number of rejected incoming (**Incoming**) or outgoing (**Outgoing**) packets.
Encrypted	Shows the number of IPSec protected incoming (**Incoming**) or outgoing (**Outgoing**) packets.
Errors	Shows the number of incoming (**Incoming**) or outgoing (**Outgoing**) packets for which the processing led to errors.

21.3 Interfaces

21.3.1 Statistics

In the **Monitoring** -> **Interfaces** -> **Statistics** menu, the current values and activities of all device interfaces are shown.

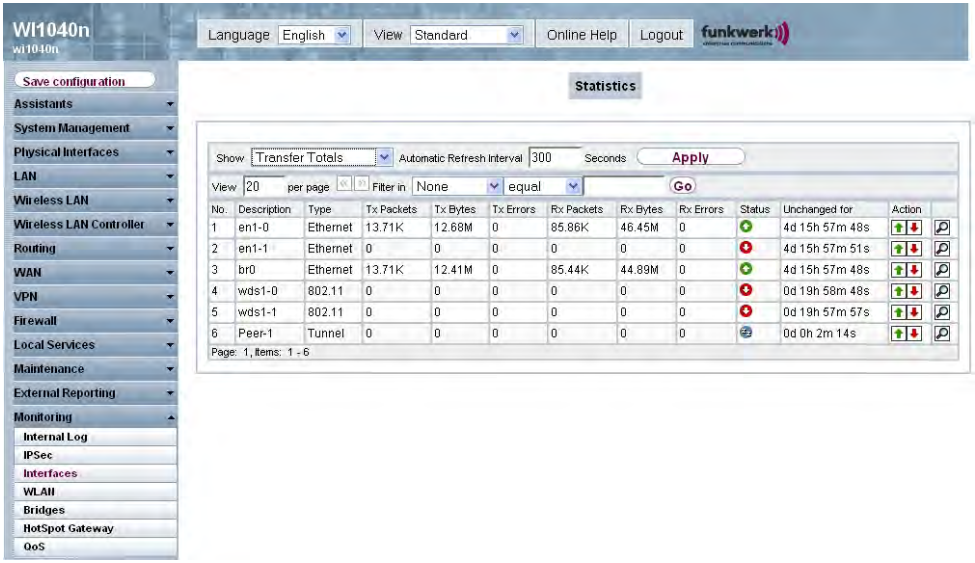


Fig. 173: **Monitoring** -> **Interfaces** -> **Statistics**

You change the state of the interface by pressing the button or button in the **Action** column. Press the button to display the statistical data for the individual interfaces in detail.

Values in the list Statistics

Field	Description
No.	Shows the serial number of the interface.
Description	Displays the name of the interface.
Type	Displays the interface text.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Tx Errors	Shows the total number of errors sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.
Rx Errors	Shows the total number of errors received.
Status	Shows the operating status of the selected interface.
Unchanged for	Shows the length of time for which the operating status of the interface has not changed.
Action	Enables you to change the status of the interface as displayed.

21.4 WLAN

21.4.1 WLAN1

In the **Monitoring** -> **WLAN** -> **WLAN1** menu, the current values and activities of the first interface are shown.

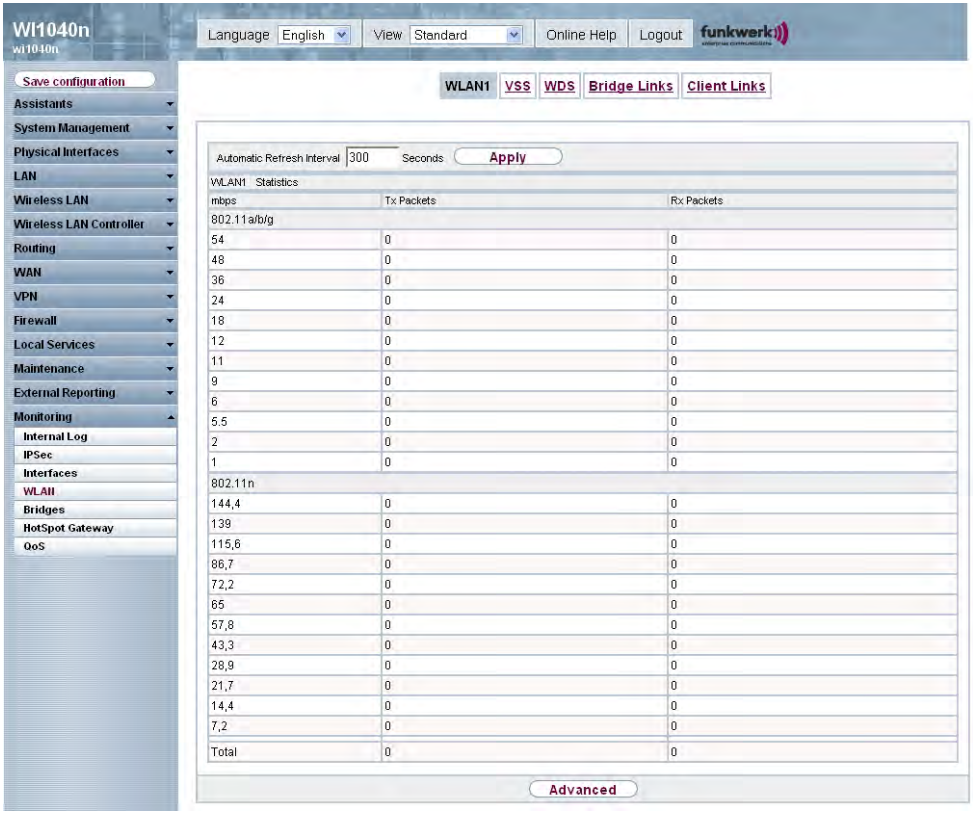


Fig. 174: **Monitoring -> WLAN -> WLAN1**

Values in the list WLAN1

Field	Description
mbps	Displays the possible data rates on this wireless module.
Tx Packets	Shows the total number of packets sent for the data rate shown in **mbps**.
Rx Packets	Shows the total number of packets received for the data rate shown in **mbps**.

You can choose the **Advanced** button to go to an overview of more details.

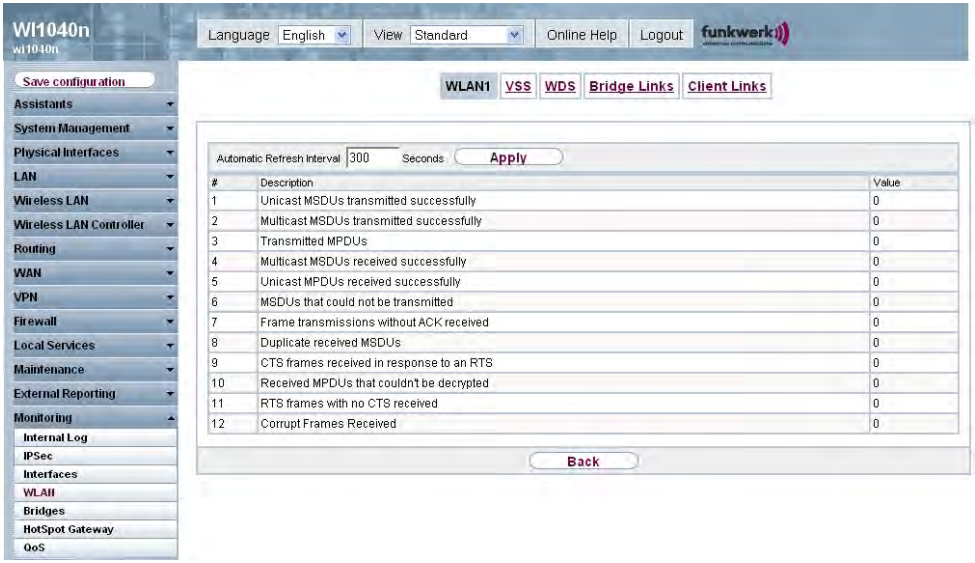


Fig. 175: **Monitoring** -> **WLAN** -> **WLAN1** -> **Advanced***menu*

Values in the list Advanced

Field	Description
#	Displays the serial number of the list entry.
Description	Displays the description of the displayed value.
Value	Displays the statistical value.

Meaning of the list entries

Description	Meaning
Unicast MSDUs transmitted successfully	Displays the number of MSDUs successfully sent to unicast addresses since the last reset. An acknowledgement was received for each of these packets.
Multicast MSDUs transmitted successfully	Displays the number of MSDUs successfully sent to multicast addresses (including the broadcast MAC address).
Transmitted MPDUs	Displays the number of MPDUs received successfully.
Multicast MSDUs received successfully	Displays the number of successfully received MSDUs that were sent with a multicast address.
Unicast MPDUs received successfully	Displays the number of successfully received MSDUs that were sent with a unicast address.
MSDUs that could not	Displays the number of MSDUs that could not be sent.

Description	Meaning
be transmitted	
Frame transmissions without ACK received	Displays the number of sent frames which which an acknowledgement frame was not received.
Duplicate received MSDUs	Displays the number of MSDUs received in duplicate.
CTS frames received in response to an RTS	Displays the number of received CTS (clear to send) frames that were received as a response to RTS (request to send).
Received MPDUs that couldn't be decrypted	Displays the number of received MSDUs that could not be encrypted. One reason for this could be that a suitable key was not entered.
RTS frames with no CTS received	Displays the number of RTS frames for which no CTS was received.
Corrupt Frames Received	Displays the number of frames received incompletely or with errors.

21.4.2 VSS

In the **Monitoring** -> **WLAN** -> **VSS** menu, the current values and activities of the configured wireless networks are shown.

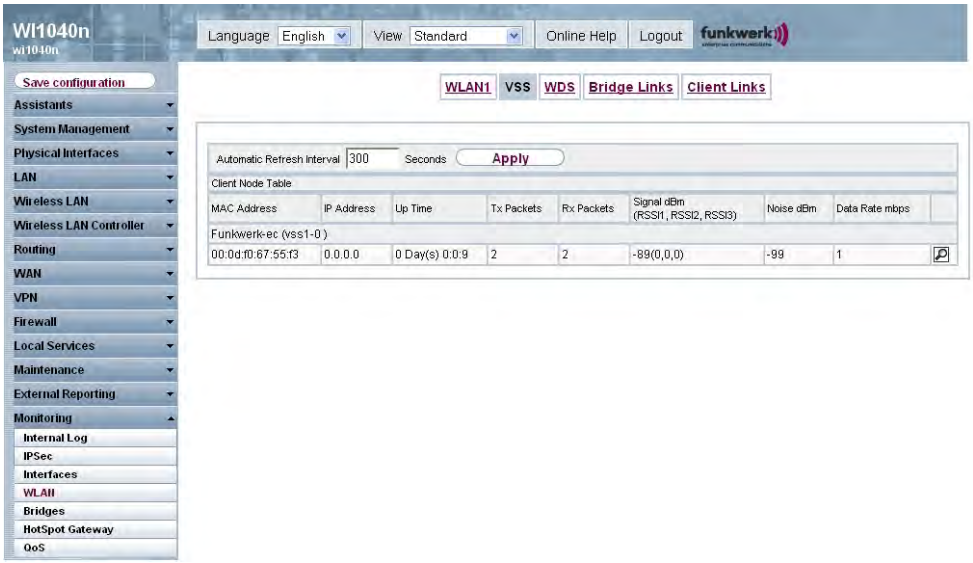


Fig. 176: **Monitoring** -> **WLAN** -> **VSS**

Values in the list VSS

Field	Description
MAC Address	Shows the MAC address of the associated client.
IP Address	Shows the IP Address of the client.
Up Time	Shows the time in hours, minutes and seconds for which the client is logged in.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.
Signal dBm	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
Data Rate mbps	Shows the current transmission rate of data received by this client in mbps. The following clock rates are possible: IEEE 802.11b: 11, 5.5, 2 and 1 mbit; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 mbit. If the 5 GHz frequency band is used, the display of 11, 5.5, 2 and 1 mbit is suppressed for IEEE 802.11b.

VSS - Details for Connected Clients

In the **Monitoring** -> **WLAN** -> **VSS** -><**Connected client**>-> menu, the current values and activities of a connected client are shown.

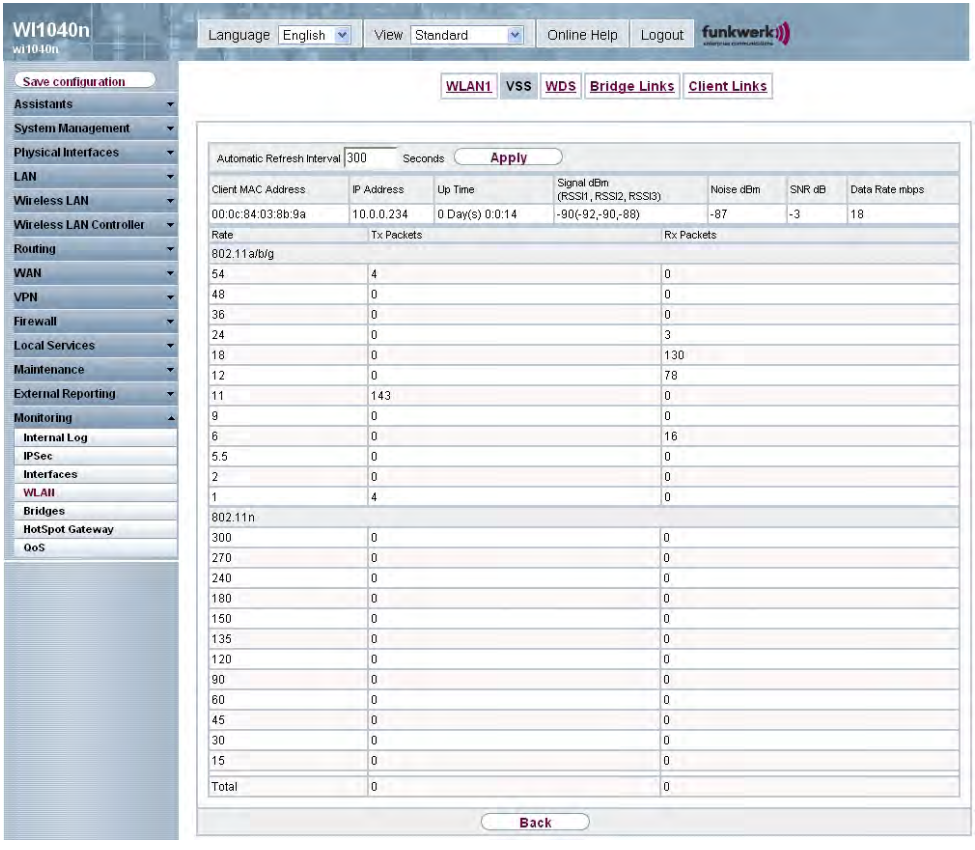


Fig. 177: **Monitoring -> WLAN -> VSS -><Connected client>->**

Values in the VSS <Connected client> list

Field	Description
Client MAC Address	Shows the MAC Address of the associated client.
IP Address	Shows the IP address of the client.
Up Time	Shows the time in hours, minutes and seconds for which the client is logged in.
Signal dBm	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
SNR dB	Signal-to-Noise Ratio in dB is an indicator of the quality of the wireless connection. Values: • > 25 dB excellent

Field	Description
	• 15 – 25 dB good • 2 – 15 dB borderline • 0 – 2 dB bad.
Data Rate mbps	Shows the current transmission rate of data received by this client in mbps. The following clock rates are possible: IEEE 802.11b: 11, 5.5, 2 and 1 mbit; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 mbit. If the 5 GHz frequency band is used, the display of 11, 5.5, 2 and 1 mbit is suppressed for IEEE 802.11b.
Rate	Displays the possible data rates on this wireless module.
Tx Packets	Shows the number of sent packets for the data rate.
Rx Packets	Shows the number of received packets for the data rate.

21.4.3 WDS

In the **Monitoring** -> **WLAN** -> **WDS** menu, the current values and activities of the configured WDS links are shown.

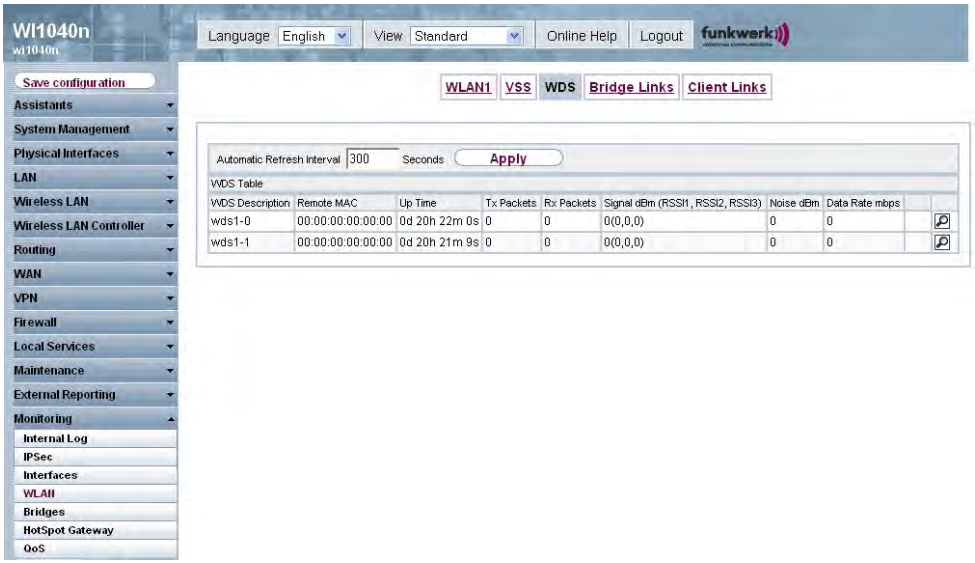


Fig. 178: **Monitoring** -> **WLAN** -> **WDS**

Values in the list WDS

Field	Description
WDS Description	Shows the name of the WDS link.
Remote MAC	Shows the MAC address of the WDS link partner.
Up Time	Shows the time in hours, minutes and seconds for which the WDS link is active.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.
Signal dBm	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
Data Rate mbps	Shows the current transmission rate of data received on this WDS link in mbps.

If required, the **Test** link can be used to start a link test. The test is only available for **funkwerk** devices and only if the WDS link is active.

The link test provides all the data necessary for checking the quality of the WDS link. The link test also helps you to align the antennas. This option is only displayed if the link is enabled.

WDS Link Details

You use the icon to open an overview of further details for the WDS links.

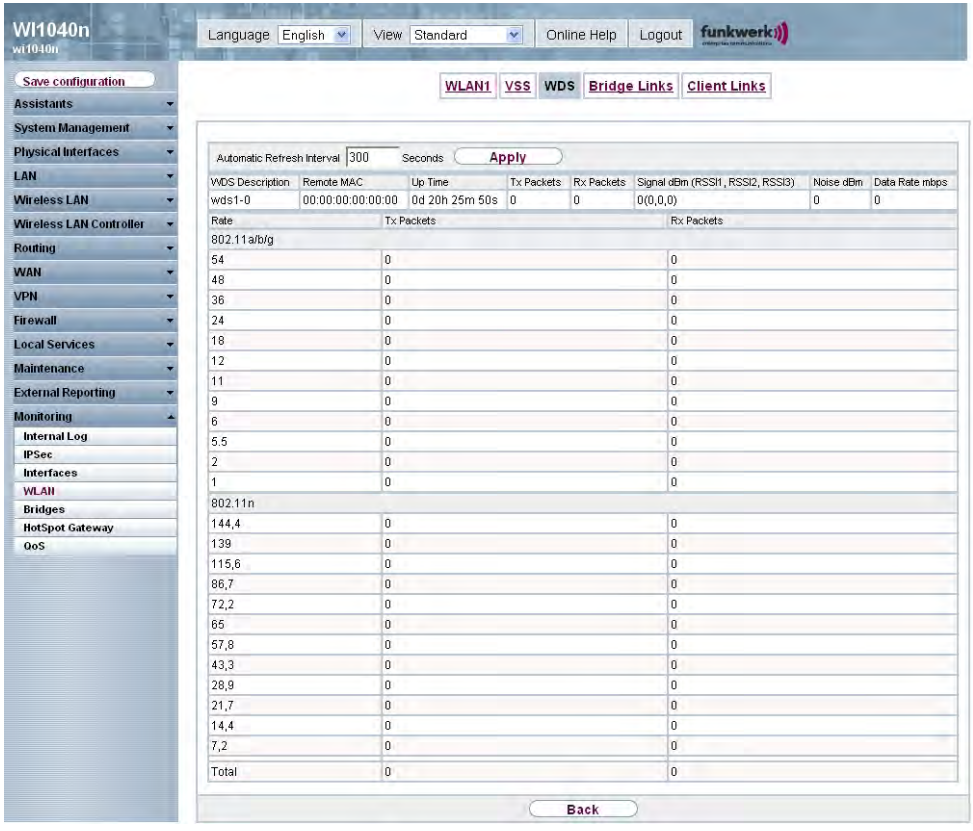


Fig. 179: **Monitoring** -> **WLAN** -> **WDS**->

Values in the WDS list

Field	Description
WDS Description	Shows the name of the WDS link.
Remote MAC	Shows the MAC address of the WDS link partner.
Up Time	Shows the time in hours, minutes and seconds for which the WDS link is active.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.
Signal dBm	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
Data Rate mbps	Shows the current transmission rate of data received on this WDS link in mbps.
Rate	Shows separately, for each of the stated data rates, the values

Field	Description
	for **Tx Packets** and **Rx Packets**.

21.4.4 Bridge Links

In the **Monitoring** -> **WLAN** -> **Bridge Links** menu, the current values and activities of the bridge links are shown.

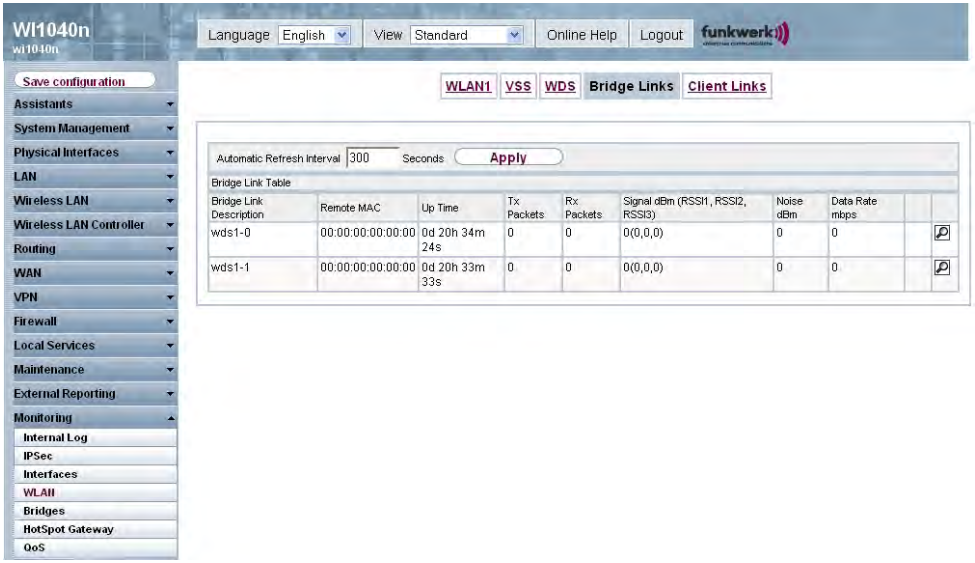


Fig. 180: **Monitoring** -> **WLAN** -> **Bridge Links**

Values in the list Bridge Links

Field	Description
Bridge Link Description	Shows the name of the bridge link.
Remote MAC	Shows the MAC address of the bridge link partner.
Up Time	Shows the time in hours, minutes and seconds for which the bridge link in question is active.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.
Signal dBm	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
Data Rate mbps	Shows the current clock rate of data received on this bridge link in mbps.

If required, the **Test** link can be used to start a link test.

The link test provides all the data necessary for checking the quality of the bridge link. The link test also helps you to align the antennas. This option is only displayed if the link state is *Enabled*.

Bridge link details

You can use the icon to open an overview of further details of the bridge links.

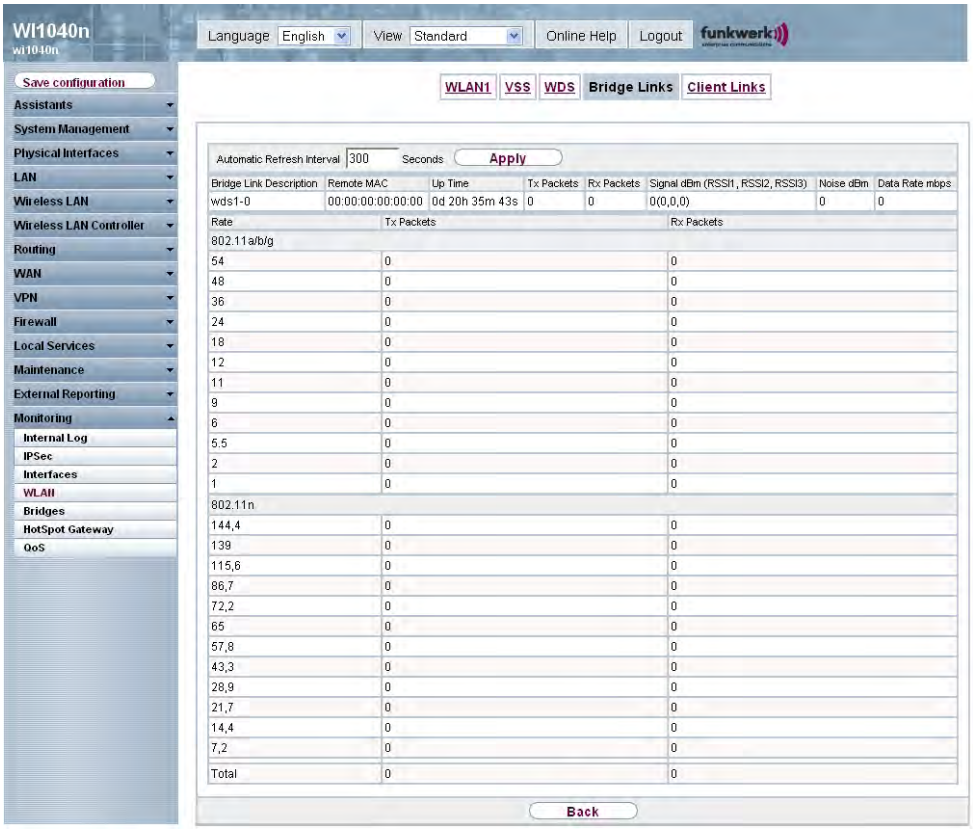


Fig. 181: **Monitoring -> WLAN -> Bridge Links->**

Values in the Bridge Links list

Field	Description
Bridge Link Description	Shows the name of the bridge link.
Remote MAC	Shows the MAC address of the bridge link partner.
Up Time	Shows the time in hours, minutes and seconds for which the

Field	Description
	bridge link in question is active.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.
Signal dBm	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
Data Rate mbps	Shows the current clock rate of data received on this bridge link in mbps.
Rate	Shows separately, for each of the stated data rates, the values for **Tx Packets** and **Rx Packets**.

21.4.5 Client Links

In the **Monitoring** -> **WLAN** -> **Client Links** menu, the current values and activities of the client links are shown.

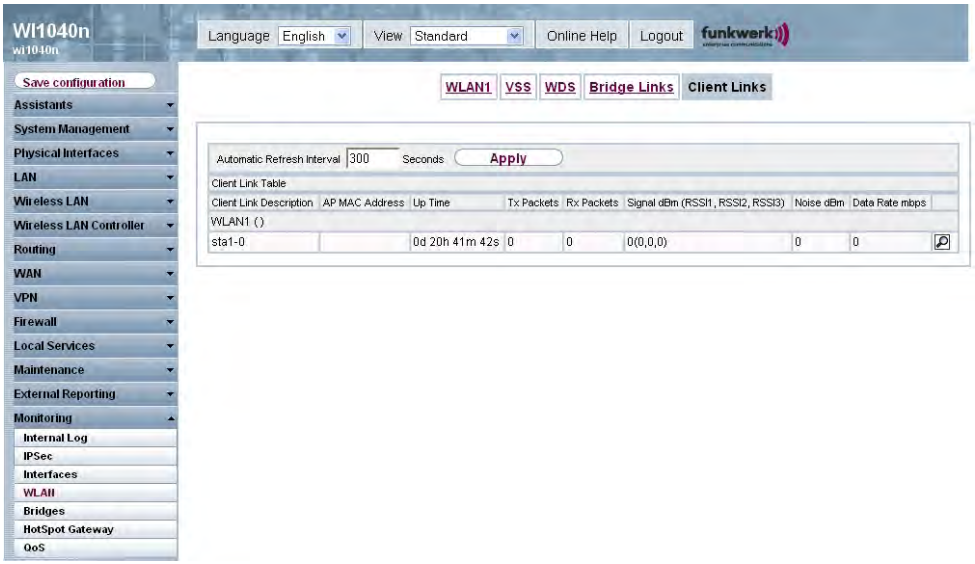


Fig. 182: **Monitoring** -> **WLAN** -> **Client Links**

Values in the Client Links list

Field	Description
Client Link Description	Shows the name of the client link.
AP MAC Address	Shows the MAC address of the client link partner.
Up Time	Shows the time in hours, minutes and seconds for which the cli-

Field	Description
	ent link in question is active.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.
Signal dBm	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
Data Rate mbps	Shows the current transmission rate of data received on this client link in mbps.

Client Link Details

You can use the icon to open an overview of further details of the client links.

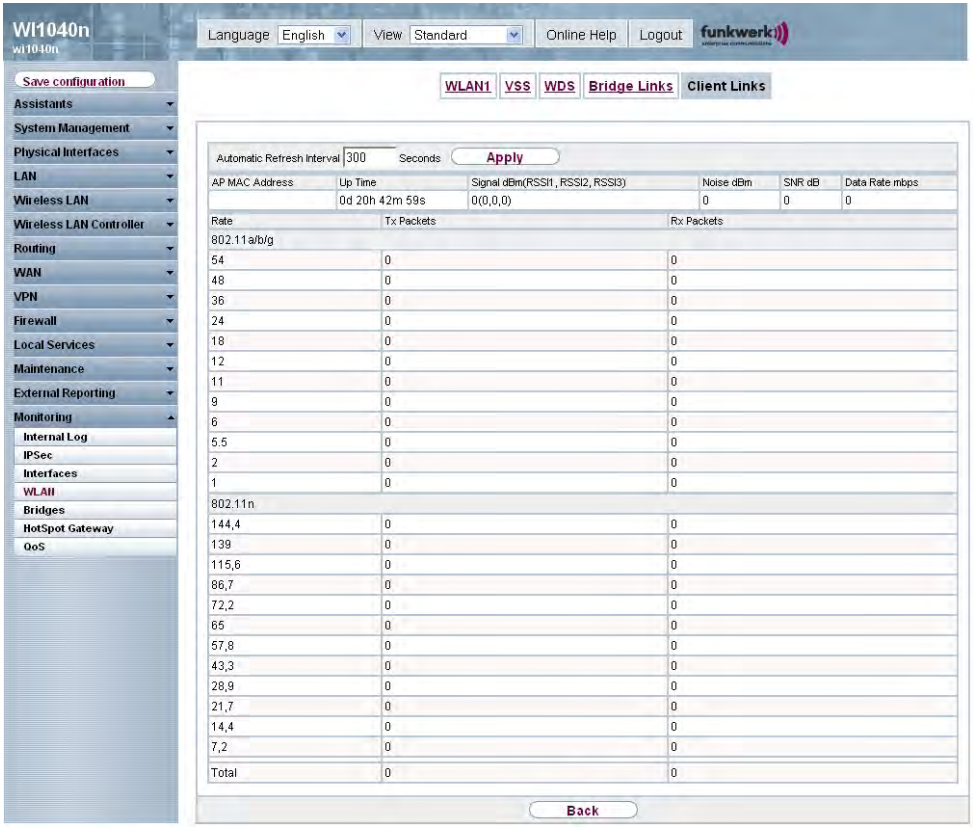


Fig. 183: **Monitoring -> WLAN -> Client Links ->**

Values in the Client Links list

Field	Description
AP MAC Address	Shows the MAC address of the client link partner.
Up Time	Shows the time in hours, minutes and seconds for which the client link in question is active.
Signal dBm	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
SNR dB	Shows the signal quality in dB.
Data Rate mbps	Shows the current transmission rate of data received on this client link in mbps.
Rate	Shows separately, for each of the stated data rates, the values for **Tx Packets** and **Rx Packets**.

21.5 Bridges

21.5.1 br<x>

In the **Monitoring** -> **Bridges** -> **br<x>** menu, the current values of the configured bridges are shown.

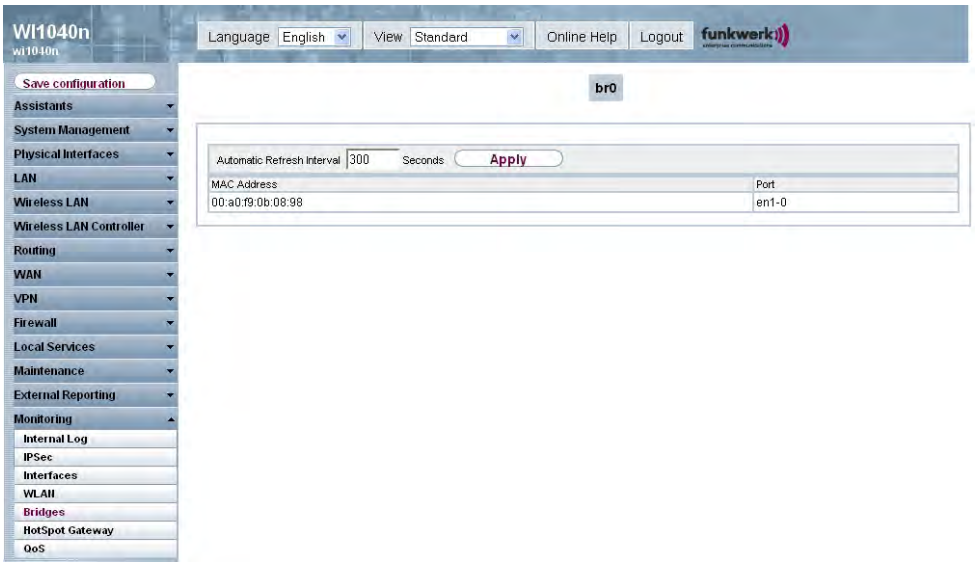


Fig. 184: **Monitoring** -> **Bridges**

Values in the br<x> list

Field	Description
MAC Address	Shows the MAC addresses of the associated bridge.
Port	Shows the port on which the bridge is active.

21.5.2 sta<x>

In the **Monitoring** -> **Bridges** -> **sta<x>** menu, the current values of the bridges to the configured WLAN clients are shown.

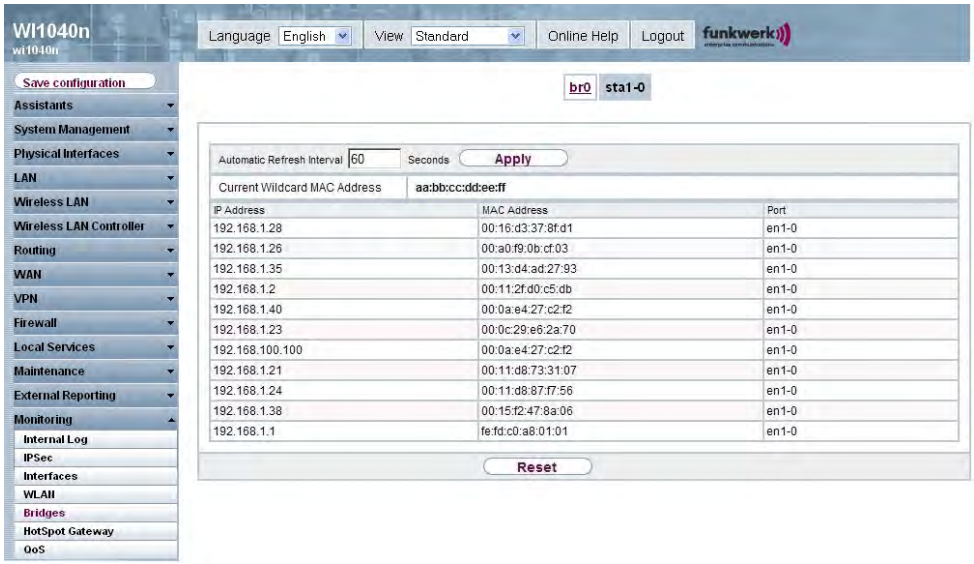


Fig. 185: **Monitoring** -> **Bridge**

Values in the sta<x> list

Field	Description
Current Wildcard MAC Address	Shows the current configured wildcard MAC address.
IP Address	Shows the IP address of the host associated with this WLAN client link.
MAC Address	Shows the MAC address of the host associated with this WLAN client link.
Port	Shows the port on which the bridge is active.

21.6 Hotspot Gateway

21.6.1 Hotspot Gateway

In the **Monitoring** -> **Hotspot Gateway** -> **Hotspot Gateway** menu, a list of all connected hosts is shown.

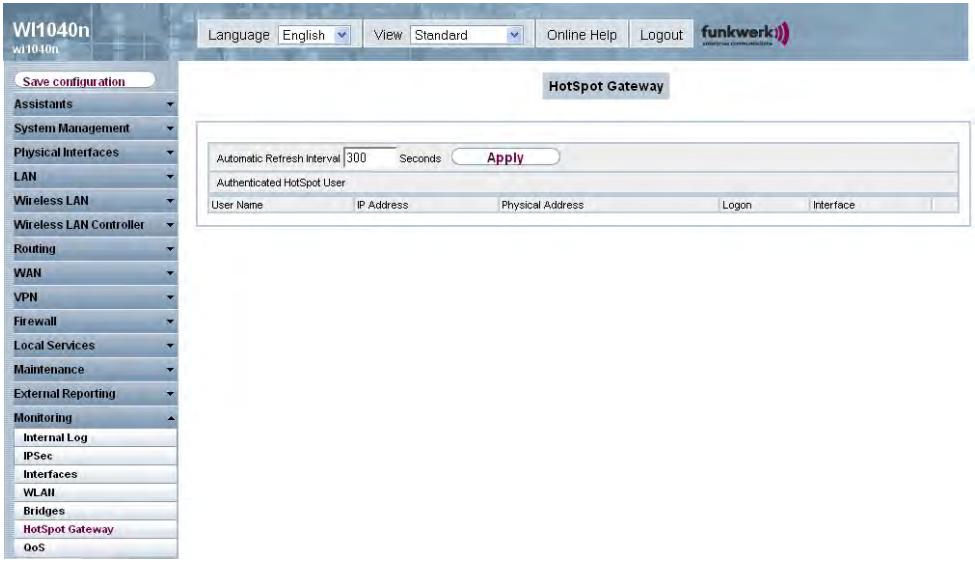


Fig. 186: **Monitoring** -> **Hotspot Gateway** -> **Hotspot Gateway**

Values in the list Hotspot Gateway

Field	Description
User Name	Displays the user's name.
IP Address	Shows the IP address of the user.
Physical Address	Shows the physical address of the user.
Logon	Shows the login time.
Interface	Shows the interface used.

21.7 QoS

In the **Monitoring** -> **QoS** menu, statistics are displayed for all interfaces for which QoS has been configured.

21.7.1 QoS

In the **Monitoring** -> **QoS** -> **QoS** menu, a list of all interfaces is shown for which QoS has been configured.

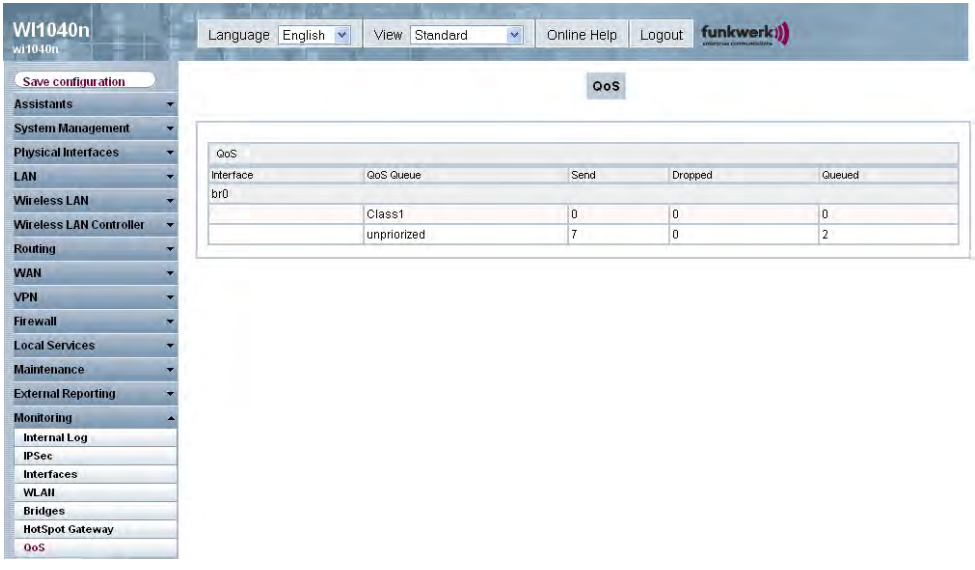


Fig. 187: **Monitoring** -> **QoS** -> **QoS**

Values in the QoS list

Field	Description
Interface	Shows the interface for which QoS has been configured.
QoS Queue	Shows the QoS Queue, which has been configured for this interface.
Send	Shows the number of sent packets with the corresponding packet class.
Dropped	Shows the number of rejected packets with the corresponding packet class in case of overloading.
Queued	Shows the number of waiting packets with the corresponding packet class in case of overloading.

Index

193

#

91 , 390 , 397
#1, #2, #3 119

A

ACCESS_ACCEPT 102
ACCESS_REJECT 102
ACCESS_REQUEST 102
ACCOUNTING_START 102
ACCOUNTING_STOP 102
ACL Mode 161 , 203
Action 168 , 168 , 176 , 176 , 207 , 309 , 353 , 371 , 390 , 395
Active IPSec Tunnels 76
Active Radio Profile 190
Active Sessions (SIF, RTP, etc...) 76
Address 316
Address Mode 133
Address Range 316
Address Type 316
Administrative Status 188 , 270
ADSL Logic 371
Alert Service 380
Alive Check 105 , 279 , 284 , 391
All Multicast Groups 235
Allow deleting/editing all routing entries 216
Allowed Addresses 161 , 203
Allowed Hotspot Client 365
Always on 260 , 297
Always on 255
AP MAC Address 168 , 406 , 407
Apply QoS 309
ARP Processing 158 , 200
Assigned Wireless Networks (VSS) 190
Authentication 258 , 262 , 299
Authentication for PPP Dialin 111
Authentication Method 275 , 391
Authentication Password 357
Authentication Type 103 , 108
Autosave Mode 119

B

Back Route Verify 215 , 273
Bandwidth 144 , 193
Based on Ethernet Interface 133
Baudrate 127
Beacon Period 150 , 196
Block after connection failure for 258 , 262 , 299
Block Time 109 , 279
blocked 253
BOSS 371
BOSS Version 76
Bridge Link Description 174 , 176 , 404 , 405
Burst Mode 148 , 195
Burst size 250
Byte Count 129
Bytes 391

C

CA Certificate 115
CA Certificates 279
Cache Hitrate (%) 332
Cache Hits 332
Cache Size 325
CAPWAP Encryption 188
Certificate is CA Certificate 113
Certificate Request Description 115
Certificate Revocation List (CRL) Checking 113
Channel 144 , 168 , 190
Channel Plan 150 , 196
Channel Sweep 152
Class ID 245 , 250
Class map 245
Clear Serial RX-Buffer 130
Clear Serial TX-Buffer 130
Client Link Description 168 , 406

Client Mode 144
Code 318
Common Name 117
Compression 97
Configuration Encryption 371
Configuration Interface 91
Configured Speed / Mode 125
Confirm Admin Password 81
Connected 168 , 176
Connection Idle Timeout 255 , 260 , 297
Connection State 242
Connection Type 297
Consider 232
Contact 79
Control Mode 247 , 266
Controlled Interfaces 349
Corrupt Frames Received 397
COS filter (802.1p/Layer 2) 242
Country 117
CPU Usage 76
Create NAT Policy 257 , 261 , 298
CTS frames received in response to an RTS 397
Current File Name in Flash 371
Current Local Time 84
Current Speed / Mode 125
Current Wildcard MAC Address 409
Custom 117
CW Max 196
CW Min 196

D

Data Bits 127
Data Packets Sequence Numbers 295
Data Rate mbps 398 , 400 , 401 , 403 , 404 , 405 , 406 , 407
Date 389
Default Route 257 , 261 , 271 , 298 , 304
Default Route Distribution 228
Delete complete IPSec configuration 289
Description 113 , 123 , 193 , 218 , 242 , 245 , 250 , 255 , 260 , 270 , 275 , 282 , 286 , 293 , 297 , 304 , 315 , 316 , 318 , 318 , 321 , 342 , 344 , 390 , 391 , 395 , 397
Destination 309
Destination File Name 371
Destination Interface 235
Destination IP Address 355 , 391
Destination IP Address / Netmask 211 , 219 , 242
Destination Port 212
Destination Port Range 318
Destination Port/Range 219 , 242
Details 390
DH Group 275
DHCP Broadcast Flag 135
DHCP Hostname 135
DHCP MAC Address 135
DHCP Options 340
DHCP Server 185
Direction 227 , 245
Distribution Mode 232
Distribution Policy 232
Distribution Ratio 233
DNS Hostname 327
DNS Negotiation 258 , 262 , 301
DNS Requests 332
DNS Server 329
DNS Server Configuration 324
DNS Test 368
Domain 329
Domain at the HotSpot Server 363
Domain Name 324
dormant 253
down 253
Drop non-members 139
Drop untagged frames 139
Dropped 394 , 411
Dropping algorithm 252
DSA Key Status 99
DSCP / TOS Value 212
DSCP/TOS filter (Layer 3) 242
DTIM Period 150 , 196

Duplicate received MSDUs 397
Dynamic RADIUS Authentication 290

E

E-mail 117
EAP Preauthentification 159 , 201
ED Threshold 196
Enable Discovery Server 359
Enable IPSec 289
Enable update 335
Enable VLAN 140
Encrypted 394
Encryption 109 , 299
Encryption Algorithms 98
Entry active 103 , 108
Errors 391 , 394
Extended Route 211
External Filename 120 , 121

F

Facility 376
Fallback interface to get DNS server 325
File Encoding 120 , 121
Filename 371
Filter 245
Filter Rules 312
Firewall Status 313
First Timeserver 84
Force certificate to be trusted 113
Forward to 329
Forwarded Requests 332
Forwarding 329
Fragmentation Threshold 150 , 152 , 196
Frame transmissions without ACK received 397

G

Garbage Collection Timer 230
Gateway 211 , 340 , 357
Generate Private Key 115
Group Description 103 , 232
Group ID 349

H

Handshake 127
Hashing Algorithms 98
Hello Interval 295
High Priority Class 245
Hold Down Timer 230
Host 329
Host for multiple locations 366
Host Name 335
HTTP 95
HTTPS 95
HTTPS TCP Port 333

I

IEEE 802.11d Compliance 144
IGMP Proxy 239
IGMP State Limit 237 , 240
IGMP Status 240
Ignore Certificate Request Payloads 291
IKE (Phase1) 393
IKE (Phase1) SAs 391
Include certificates and keys 371
Inter-Byte Gap 129
Interface 93 , 96 , 125 , 139 , 185 , 211 , 215 , 218 , 227 , 233 , 237 , 247 , 266 , 312 , 329 , 335 , 339 , 351 , 353 , 357 , 363 , 410 , 411
Interface Action 351
Interface Description 91
Interface Mode 133
Interfaces 245
Internal Timeserver 84
Interval 349 , 355
Intra-cell Repeating 158 , 200
Invalid DNS Packets 332
IP Accounting 378
IP accounting message format 379
IP Address 227 , 327 , 342 , 357 , 376 , 386 , 398 , 400 , 409 , 410
IP Address Assignment 271

IP Address Mode 257 , 261 , 298
IP Address Range 185 , 339
IP address to use for DNS/WINS server assignment 325
IP Address/Netmask 133
IP Assignment Pool 271
IP Assignment Pool (IPCP) 298
IP Compression 284
IP Pool Name 265 , 288
IP Pool Range 265 , 288
IPSec (Phase2) 393
IPSec (Phase2) SAs 391
IPSec Debug Level 289
IPSec Tunnels 393

K

Key Value 304

L

Language for login window 363
Last Member Query Interval 237
Last Write Result 357
Layer 4 Protocol 212
LCP Alive Check 258 , 262 , 299
LDAP URL Path 123
Lease Time 340
Level 376 , 389
Licence Key 88
Licence Serial Number 88
Lifetime 275 , 282
Local Certificate 275 , 333
Local Certificate Description 120 , 121
Local GRE IP Address 304
Local Hostname 293
Local ID 391
Local ID Type 275
Local ID Value 275
Local IP Address 129 , 211 , 257 , 261 , 271 , 295 , 298 , 304 , 391
Local Port 129 , 391
Local PPTP IP Address 262
Locality 117
Location 79 , 188
Logged Actions 313
Logging Level 97
Logon 410
Long Retry Limit 150 , 152 , 196

M

MAC Address 133 , 342 , 357 , 398 , 400 , 408 , 409
Mail Exchanger (MX) 336
Management VID 140
Matching String 382
Max Receive Lifetime 196
Max Transmit MSDU Lifetime 196
Max. Clients 158 , 200
Max. Link Distance 144
Max. queue size 252
Max. Scan Duration 176
Max. Time Period for Active Scan 152
Max. Time Period for Passive Scan 152
Max. Transmission Rate 148 , 195
Maximum Groups 240
Maximum Message Level of Syslog Entries 79
Maximum Messages per Minute 380
Maximum Number of Accounting Log Entries 79
Maximum Number of Dialup Retries 258 , 262
Maximum Number of Syslog Entries 79
Maximum Response Time 237
Maximum Retries 295
Maximum Sources 240
Maximum Time between Retries 295
Maximum TTL for Negative Cache Entries 325
Maximum TTL for Positive Cache Entries 325
Maximum Upload Speed 247 , 250 , 266
mbps 396
Members 315 , 321

Memory Usage 76
Message 389
Message Compression 382
Message Timeout 382
Messages 391
Metric 211
Metric Offset for Active Interfaces 227
Metric Offset for Inactive Interfaces 227
Min. queue size 252
Min. Time Period for Active Scan 152
Min. Time Period for Passive Scan 152
Minimum Time between Retries 295
Mode 115 , 129 , 168 , 212 , 215 , 237 , 240 , 275 , 286
Mode / Bridge Group 91
Monitored Interface 351
Monitored Interfaces 387
Monitored IP Address 349
MSDUs that could not be transmitted 397
MTU 304 , 391
Multicast Group Address 235
Multicast MSDUs received successfully 397
Multicast MSDUs transmitted successfully 397

N

Name 286
NAT active 217
NAT Detection 391
NAT Method 218
NAT Traversal 279
Negative Cache 325
Negotiation Type 391
Netmask 211 , 227 , 298 , 357
Network Name (SSID) 158 , 166 , 168 , 200
Network Type 211
New Destination IP Address/Netmask 221
New Destination Port 221
New File Name 371
New Source Port 221
No. 215 , 389 , 395
Node Name 357
Noise dBm 398 , 400 , 401 , 403 , 404 , 405 , 406 , 407
Number of Admitted Connections 272
Number of Messages 382
Number of Spatial Streams 144 , 193

O

Operation Band 144 , 193
Operation Mode 144 , 190 , 193
Organisation 117
Organisational Unit 117
OSPF Mode 301
Other Inactivity 314
Outgoing Interface 250
Overbooking allowed 250

P

Packets 391
Parity 127
Passed 394
Password 115 , 120 , 121 , 255 , 260 , 286 , 293 , 297 , 335 , 371 , 381 , 387
Peer Address 270
Peer ID 270
Phase 1 Profile 272
Phase 2 Profile 272
Physical Address 410
Physical Interface - Interface Specifics - Link 77
Ping 95
Ping Test 367
Poisoned Reverse 228
Policy 105 , 109
Pool Usage 339
POP3 Server 381
POP3 Timeout 381
Port 125 , 337 , 408 , 409
Port Mode 126 , 131

Port Number 129
Portforwardings 217
Positive Cache 325
PPPoE Ethernet Interface 255
PPPoE Interfaces for Multilink 255
PPPoE Mode 255
PPTP Address Mode 262
PPTP Inactivity 314
PPTP Interface 260
PPTP Passthrough 217
Preshared Key 159 , 163 , 166 , 175 , 201 , 270
Primary 324 , 324
Primary DHCP Server 343
Priorisation algorithm 247
Priorisation queue 250
Prioritize TCP ACK Packets 258 , 262 , 299
Priority 103 , 108 , 250 , 309
Privacy 163 , 175
Propagate PMTU 284
Proposals 275 , 282
Protocol 219 , 242 , 318 , 337 , 376
Protocol Header Size below Layer 3 247
Provider 335
Provider Name 337
Proxy ARP 135 , 273
Proxy ARP Mode 301
Proxy Interface 239
PVID 139

Q

QoS Queue 411
Query Interval 237
Queued 411
Queues/Policies 247

R

RA Encrypt Certificate 115
RA Sign Certificate 115
RADIUS Dialout 105
RADIUS Password 103
RADIUS Server 201
RADIUS Server Group ID 286
Rate 403 , 405 , 407
Real Time Jitter Control 247
Receive Version 224
Received DNS Packets 332
Received MPDUs that couldn't be decrypted 397
Recent System Logs 77
Recipient 382
Region 177 , 185
Remote Configuration 174
Remote Device Name 176
Remote GRE IP Address 304
Remote Hostname 293
Remote ID 391
Remote IP 129
Remote IP Address 294 , 390
Remote Link Description 176
Remote Link Enabled 176
Remote MAC 401 , 403 , 404 , 405
Remote MAC Address 165 , 175 , 176
Remote Networks 390
Remote Port 391
Remote PPTP IP Address 262
Response 327
Retransmission Timer 230
Retries 105
RFC 2091 Variable Timer 228
RFC 2453 Variable Timer 228
RIP UDP Port 228
Roaming Profile 152
Robustness 237
Role 286
Route Announce 224
Route Entries 257 , 261 , 271 , 298 , 304
Route Timeout 230
Route Type 211
RSA Key Status 99
RTS frames with no CTS received 397
RTS Threshold 150 , 152 , 196

RTT Mode (Realtime Traffic Mode) 250
Rx Bytes 395
Rx Errors 395
Rx Packets 395 , 396 , 398 , 400 , 401 , 403 , 404 , 405 , 406

S

Scan channels 152
Scan Interval 152
Scan Threshold 152
SCEP URL 115
Schedule Interval 348
Second Timeserver 84
Secondary 324 , 324
Secondary DHCP Server 343
Security Algorithm 390
Security Mode 159 , 166 , 201
Select action 344
Select file 371
Select interface 344
Select radio 344
Selected Channel 144
Selection 318
Send 411
Send Certificate Chains 291
Send Certificate Request Payloads 291
Send CRLs 291
Send information to 387
Send Initial Contact Message 290
Send Key Hash Payloads 291
Send Version 224
Sender E-Mail Address 380
Serial Number 76
Server 337
Server Failures 332
Server IP Address 103 , 108
Server Timeout 105
Service 219 , 309
Set Date 84
Set Time 84
Severity 382
SHDSL Logic 371
Short Guard Internal 150
Short Guard Interval 152 , 196
Short Retry Limit 150 , 152 , 196
Show passwords and keys in clear text 82
Signal 168
Signal dBm 176 , 398 , 400 , 401 , 403 , 404 , 405 , 406 , 407
Silent Deny 217
SMTP Authentication 381
SMTP Server 381
SNMP 95
SNMP Listen UDP Port 100
SNMP Read Community 81
SNMP Trap Broadcasting 384
SNMP Trap Community 384
SNMP Trap UDP Port 384
SNMP Version 100
SNMP Write Community 81
SNR dB 400 , 407
Source 309
Source File Name 371
Source Interface 212 , 235
Source IP Address 349 , 355
Source IP Address / Netmask 212 , 219 , 221 , 242
Source Location 207 , 344 , 371
Source Port 212 , 219
Source Port Range 318
Source Port/Range 219 , 242
Specify bandwidth 312
SSH 95
SSH service active 97
Start Mode 272
Start Time 346
State/Province 117
Status 390 , 393 , 395
Stop Bits 127
Stop Time 346
Subnet 316
Subsystem 383 , 389
Successfully Answered Queries 332
Summary 117
Sync SAs with ISP interface state 290

System Admin Password 81
System Date 76
System Logic 371
System Name 79

T

TACACS+ Secret 108
TCP Inactivity 314
TCP Keepalives 97
TCP Port 109
TCP-MSS Clamping 135
Telnet 95
Temperature 76
Terms & Conditions 363
TFTP File Name 344
TFTP Server 344
Third Timeserver 84
Ticket Type 365
Time 389
Time Condition 346
Time Update Interval 84
Time Update Policy 84
Time Zone 84
Timeout 109 , 129
Timestamp 376
Total 394
Traceroute Test 368
Traffic shaping 247 , 250 , 312
Transmit Key 159 , 163 , 166 , 201
Transmit Power 144 , 190
Transmitted MPDUs 397
Transparent MAC Address 93
Trials 349
Trigger 351 , 353
TTL 327
Tunnel Profile 297
Tx Bytes 395
Tx Errors 395
Tx Packets 395 , 396 , 398 , 400 , 401 , 403 , 404 , 405 , 406
Type 242 , 318 , 395
Type of Messages 376
Type of traffic 218

U

UDP Destination Port 294 , 302 , 387
UDP Inactivity 314
UDP Port 105
UDP Source Port 294
UDP Source Port Selection 302
Unchanged for 395
Unicast MPDUs received successfully 397
Unicast MSDUs transmitted successfully 397
up 253
Up Time 398 , 401 , 403 , 404 , 406 , 407
Update Interval 337 , 387
Update Path 337
Update Timer 230
Update URL 344
UpT ime 405
Upt Tme 400
Uptime 76
URL 207 , 371
Usage Area 144
Use key 304
Use PFS Group 282
Use Zero Cookies 290
Used Channel 190
Used Secondary Channel 144
User Defined Channel Plan 196
User Name 255 , 260 , 297 , 335 , 381 , 410
Users 286

V

Value 397
Vendor Mode 103
VLAN 204
VLAN ID 133 , 204
VLAN Identifier 138
VLAN Members 138
VLAN Name 138

W

Walled Garden 363
Walled Garden URL 363
Walled Network / Netmask 363
WDS Description 163 , 401 , 403
Weight 250
WEP Key 1 - 4 163
WEP Key 1-4 159 , 166 , 201
Wildcard 336
Wildcard MAC Address 93
Wildcard Mode 93
Wireless Mode 148 , 195
WMM 158 , 200
WPA Cipher 159 , 166 , 201
WPA Mode 159 , 166 , 201
WPA2 Cipher 159 , 166 , 201

X

XAUTH Profile 272

Z

Zero Cookie Size 290